

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики
Мегафакультет трансляционных информационных технологий
Факультет информационных технологий и программирования

Лабораторная работа №7
По дисциплине «Телекоммуникационные системы и технологии»
DNS

Выполнили студенты группы М33081
Аль Даббагх Харит Хуссейн

Мазумдер Шоувик

Миах Такбир

Проверила
Шараева Кристина Витальевна

САНКТ-ПЕТЕРБУРГ

2022

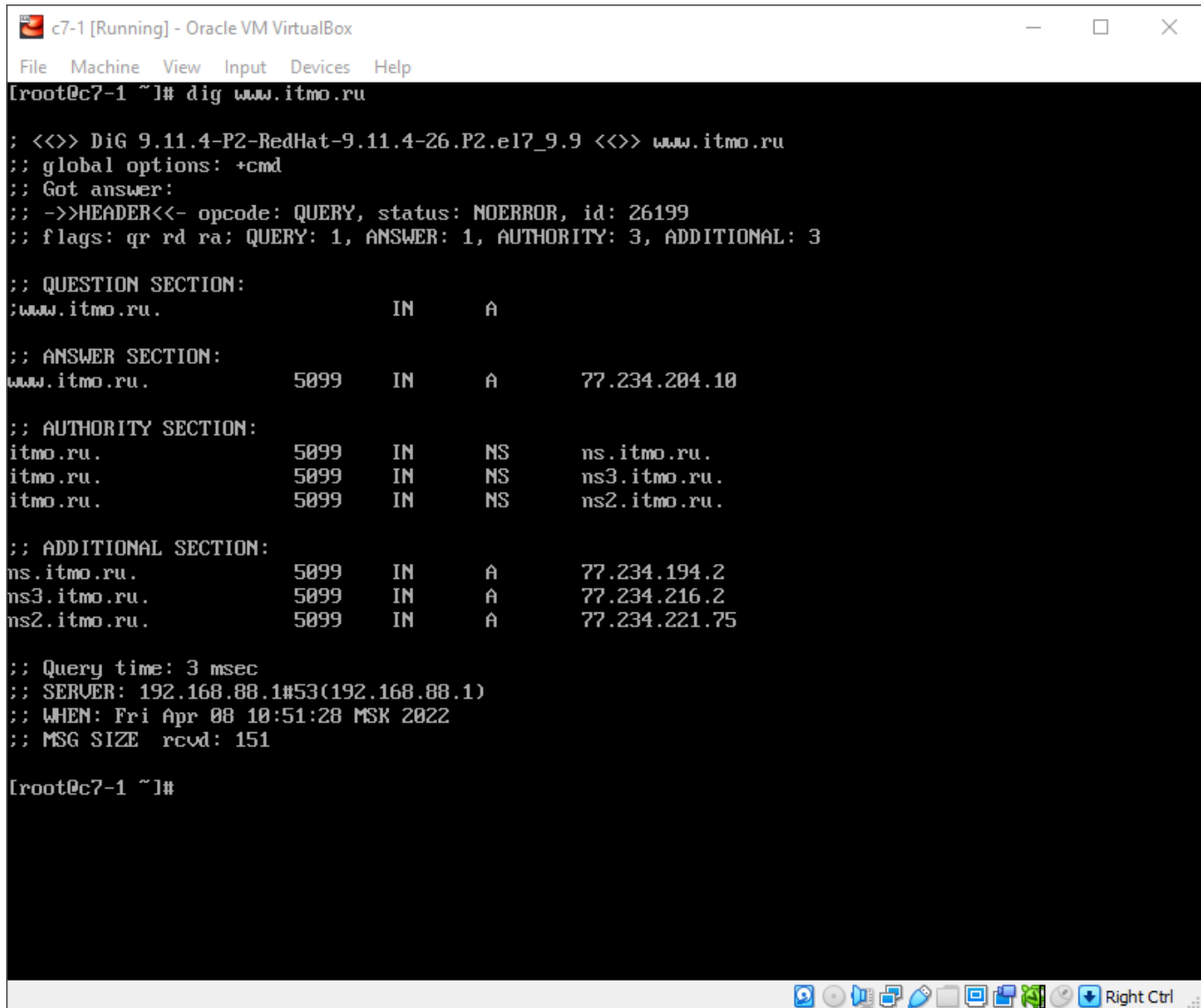
СОДЕРЖАНИЕ

Артефакты	2
Вопросы и задания.....	10

АРТЕФАКТЫ

Часть 2. Получение информации из DNS с помощью утилиты dig

1. На хосте c7-1 с выполните команду `dig www.itmo.ru`. В консольном выводе изучите состав секций HEADER, QUESTION SECTION, ANSWER SECTION, AUTHORITY SECTION, SERVER: 192.168.0.1, WHEN и MSG SIZE. Соотнесите значения полей секции HEADER со значениями остальных полей. (!)



```
c7-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@c7-1 ~]# dig www.itmo.ru

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> www.itmo.ru
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 26199
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

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

;; ANSWER SECTION:
www.itmo.ru.                5099    IN      A      77.234.204.10

;; AUTHORITY SECTION:
itmo.ru.                    5099    IN      NS      ns.itmo.ru.
itmo.ru.                    5099    IN      NS      ns3.itmo.ru.
itmo.ru.                    5099    IN      NS      ns2.itmo.ru.

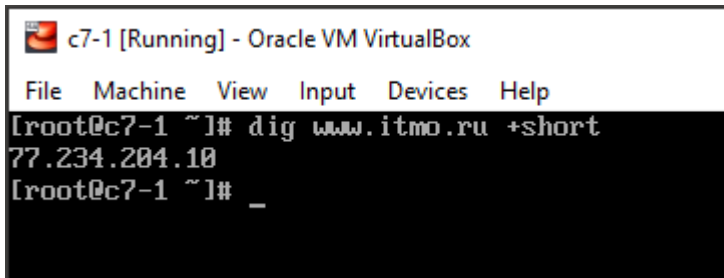
;; ADDITIONAL SECTION:
ns.itmo.ru.                 5099    IN      A      77.234.194.2
ns3.itmo.ru.               5099    IN      A      77.234.216.2
ns2.itmo.ru.               5099    IN      A      77.234.221.75

;; Query time: 3 msec
;; SERVER: 192.168.88.1#53(192.168.88.1)
;; WHEN: Fri Apr 08 10:51:28 MSK 2022
;; MSG SIZE  rcvd: 151

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

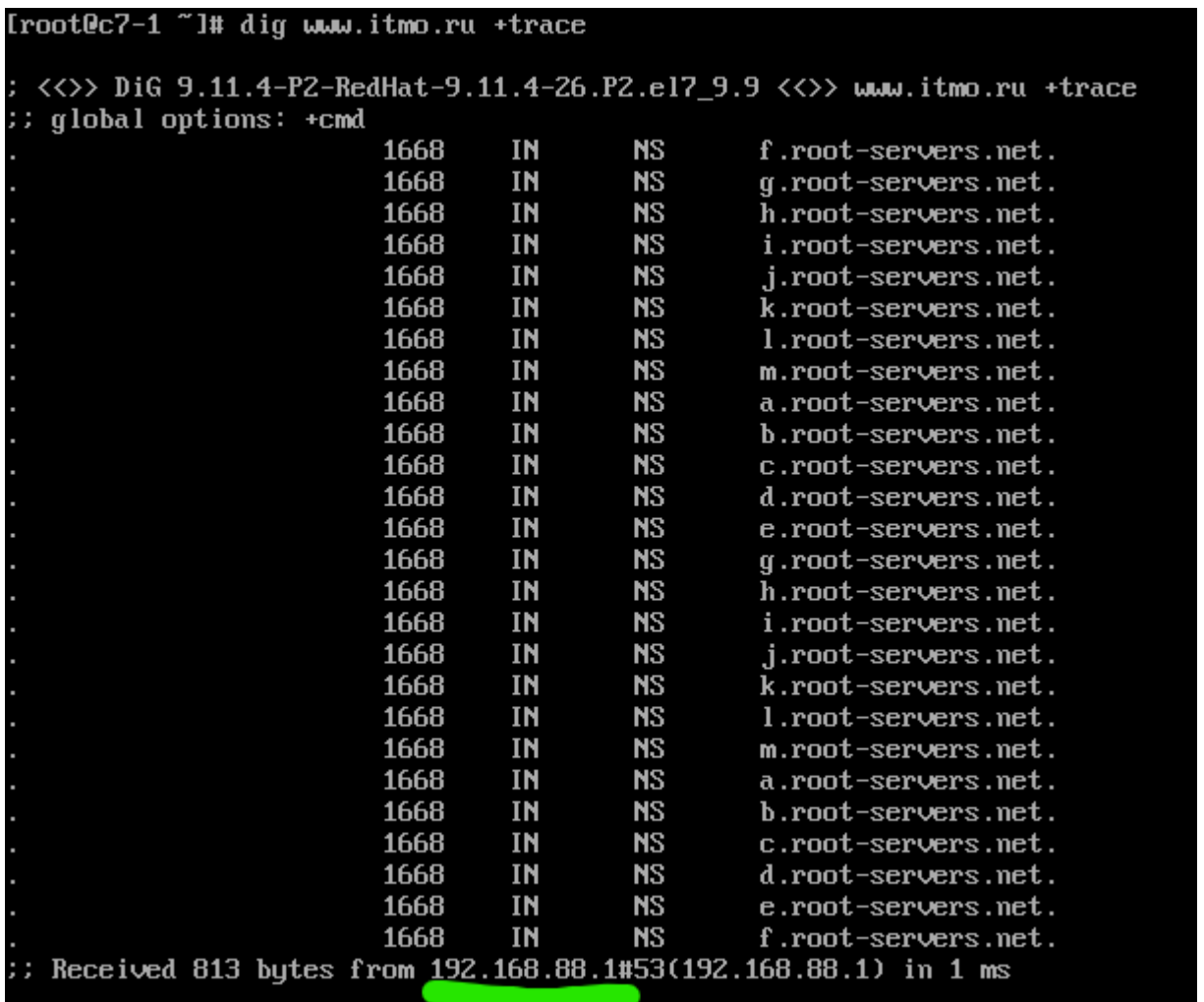
2. На хосте c7-1 с помощью утилиты dig решите следующие задачи (!):

а. Выведите только результат разрешения имени www.itmo.ru (только IP адрес),



```
c7-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@c7-1 ~]# dig www.itmo.ru +short
77.234.204.10
[root@c7-1 ~]# _
```

б. Выведите на экран подробную информацию о разрешении имени, с выводом всех промежуточных серверов, определите какой именно DNS сервер вернул IP адрес хоста.



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

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> www.itmo.ru +trace
;; global options: +cmd
.                1668      IN      NS      f.root-servers.net.
.                1668      IN      NS      g.root-servers.net.
.                1668      IN      NS      h.root-servers.net.
.                1668      IN      NS      i.root-servers.net.
.                1668      IN      NS      j.root-servers.net.
.                1668      IN      NS      k.root-servers.net.
.                1668      IN      NS      l.root-servers.net.
.                1668      IN      NS      m.root-servers.net.
.                1668      IN      NS      a.root-servers.net.
.                1668      IN      NS      b.root-servers.net.
.                1668      IN      NS      c.root-servers.net.
.                1668      IN      NS      d.root-servers.net.
.                1668      IN      NS      e.root-servers.net.
.                1668      IN      NS      g.root-servers.net.
.                1668      IN      NS      h.root-servers.net.
.                1668      IN      NS      i.root-servers.net.
.                1668      IN      NS      j.root-servers.net.
.                1668      IN      NS      k.root-servers.net.
.                1668      IN      NS      l.root-servers.net.
.                1668      IN      NS      m.root-servers.net.
.                1668      IN      NS      a.root-servers.net.
.                1668      IN      NS      b.root-servers.net.
.                1668      IN      NS      c.root-servers.net.
.                1668      IN      NS      d.root-servers.net.
.                1668      IN      NS      e.root-servers.net.
.                1668      IN      NS      f.root-servers.net.
;; Received 813 bytes from 192.168.88.1#53(192.168.88.1) in 1 ms
```

С. Выведите конфигурационную запись (SOA) домена itmo.ru, определите, значения каждого из числовых параметров записи, что они означают?

```

c7-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@c7-1 ~]# dig itmo.ru +nssearch
SOA ns.itmo.ru. hostmaster.itmo.ru. 2021011385 3600 1800 86400 3600 from server 77.234.194.2 in 25 m
s.
SOA ns.itmo.ru. hostmaster.itmo.ru. 2021011385 3600 1800 86400 3600 from server 77.234.221.75 in 25
ms.
SOA ns.itmo.ru. hostmaster.itmo.ru. 2021011385 3600 1800 86400 3600 from server 77.234.216.2 in 46 m
s.
[root@c7-1 ~]# _
  
```

2021011385	zone serial number	Когда в файле зоны меняется серийный номер, это предупреждает вторичные серверы имен о том, что они должны обновить свои копии файла зоны путем передачи зоны.
3600	REFRESH	Продолжительность времени (в секундах), в течение которого вторичные серверы должны ждать, прежде чем запрашивать у первичных серверов запись SOA, чтобы узнать, была ли она обновлена.
1800	RETRY	Продолжительность времени, в течение которого сервер должен ждать, чтобы снова запросить обновление у неответающего первичного сервера имен.
86400	EXPIRE	Если вторичный сервер не получает ответа от первичного сервера в течение этого времени, он должен прекратить отвечать на запросы для этой зоны.
3600	TTL	Интервал, через который обновляется сама запись SOA.

d. Определите, какие сервера обрабатывают почту домена itmo.ru.

```
c7-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
S.
SOA ns1.google.com. dns-admin.google.com. 440057678 900 900 1800 60 from server 216.239.36.10 in 7 m
S.
SOA ns1.google.com. dns-admin.google.com. 440057678 900 900 1800 60 from server 216.239.32.10 in 36
ms.
SOA ns1.google.com. dns-admin.google.com. 440057678 900 900 1800 60 from server 216.239.34.10 in 49
ms.
[root@c7-1 ~]# dig itmo.ru MX

;<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <>> itmo.ru MX
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 35419
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

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

;; ANSWER SECTION:
itmo.ru.                7200    IN      MX      10 emx.mail.ru.

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

;; ADDITIONAL SECTION:
ns3.itmo.ru.            1867    IN      A       77.234.216.2
ns2.itmo.ru.            1867    IN      A       77.234.221.75
ns.itmo.ru.             1867    IN      A       77.234.194.2

;; Query time: 36 msec
;; SERVER: 192.168.88.1#53(192.168.88.1)
;; WHEN: Fri Apr 08 11:45:21 MSK 2022
;; MSG SIZE rcvd: 161

[root@c7-1 ~]# _
```

e. Определите какие DNS сервера обслуживают зону itmo.ru и какие у них ip адреса.

```
c7-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
S.
SOA ns1.google.com. dns-admin.google.com. 440057678 900 900 1800 60 from server 216.239.36.10 in 7 m
S.
SOA ns1.google.com. dns-admin.google.com. 440057678 900 900 1800 60 from server 216.239.32.10 in 36
ms.
SOA ns1.google.com. dns-admin.google.com. 440057678 900 900 1800 60 from server 216.239.34.10 in 49
ms.
[root@c7-1 ~]# dig itmo.ru MX

;<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <>> itmo.ru MX
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 35419
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

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

;; ANSWER SECTION:
itmo.ru.                7200    IN      MX      10 emx.mail.ru.

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

;; ADDITIONAL SECTION:
ns3.itmo.ru.            1867    IN      A       77.234.216.2
ns2.itmo.ru.            1867    IN      A       77.234.221.75
ns.itmo.ru.             1867    IN      A       77.234.194.2

;; Query time: 36 msec
;; SERVER: 192.168.88.1#53(192.168.88.1)
;; WHEN: Fri Apr 08 11:45:21 MSK 2022
;; MSG SIZE rcvd: 161

[root@c7-1 ~]# _
```

f. Значение записи в зоне обратного просмотра для 87.250.250.242.

```
c7-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@c7-1 ~]# dig -x 87.250.250.242

;<<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> -x 87.250.250.242
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 791
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
242.250.250.87.in-addr.arpa. 95 IN      PTR      ya.ru.

;; Query time: 19 msec
;; SERVER: 192.168.88.1#53(192.168.88.1)
;; WHEN: Fri Apr 08 11:50:14 MSK 2022
;; MSG SIZE rcvd: 64

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

г. Определите количество серверов, поддерживающих корневую зону.

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

;<<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> .
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27951
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 13

;; QUESTION SECTION:
;.                                IN      A

;; AUTHORITY SECTION:
.                2690    IN      NS      f.root-servers.net.
.                2690    IN      NS      g.root-servers.net.
.                2690    IN      NS      h.root-servers.net.
.                2690    IN      NS      i.root-servers.net.
.                2690    IN      NS      j.root-servers.net.
.                2690    IN      NS      k.root-servers.net.
.                2690    IN      NS      l.root-servers.net.
.                2690    IN      NS      m.root-servers.net.
.                2690    IN      NS      a.root-servers.net.
.                2690    IN      NS      b.root-servers.net.
.                2690    IN      NS      c.root-servers.net.
.                2690    IN      NS      d.root-servers.net.
.                2690    IN      NS      e.root-servers.net.

;; ADDITIONAL SECTION:
f.root-servers.net. 602410 IN      A      192.5.5.241
g.root-servers.net. 602410 IN      A      192.112.36.4
```

Конфигурационный файл /etc/named.conf из Части 3, п.3.

```
//
// 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

acl allowed-hosts {
    10.0.0.2;
};

options {
    listen-on port 53 { 127.0.0.1; 10.0.0.0/24; };
    listen-on-v6 port 53 { none; };
    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.secreots";
    allow-query { allowed-hosts; };
    allow-query-cache { allowed-hosts; };
    allow-recursion { allowed-hosts; };
    version "My Own DNS Server";

    /*
     - 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 no;

    /* 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";
};

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";

```


c7-2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```

[root@c7-2 ~]# ping itmo.ru
PING itmo.ru (77.234.204.10) 56(84) bytes of data.
^C
--- itmo.ru ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1000ms

[root@c7-2 ~]# dig itmo.ru +short +identify
77.234.204.10 from server 10.0.0.1 in 0 ms.
[root@c7-2 ~]# dig @10.0.0.1 -c CH -t txt version.bind

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> @10.0.0.1 -c CH -t txt version.bind
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 47951
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;version.bind.                CH      TXT

;; ANSWER SECTION:
version.bind.                 0       CH      TXT      "My Own DNS Server"

;; AUTHORITY SECTION:
version.bind.                 0       CH      NS       version.bind.

;; Query time: 0 msec
;; SERVER: 10.0.0.1#53(10.0.0.1)
;; WHEN: Fri Apr 08 13:25:43 MSK 2022
;; MSG SIZE rcvd: 85

[root@c7-2 ~]# _

```

Часть 4

Параметры, добавленные в файл /etc/named.conf в Части 4. п. 3.

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

Файл зоны, созданный в Части 4.

```
;
; Bind data file for hbm.local zone
;
$TTL 300
@ IN SOA ns1.hbm.local. harith.hbm.local. (
    2022041312 ; Serial
    43200      ; Refresh
    3600       ; Retry
    3600000    ; Expire
    300 )      ; Negative Cache TTL
;
@ IN NS ns1.template.lan.

ns1 IN A 10.0.0.1
gate IN A 10.0.0.1
www IN CNAME gate.hbm.local.
```

ВОПРОСЫ И ЗАДАНИЯ

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

`HEADER`: Заголовок включает поля, определяющие, какие из остальных разделов присутствуют, а также указывает, является ли сообщение запросом или ответом, стандартным запросом или каким-то другим опкодом и т.д.

`QUESTION`: Секция вопроса используется для переноса "вопроса" в большинстве запросов, т.е. параметров, определяющих то, что спрашивается.

`ANSWER`, `AUTHORITY`: Разделы ответа и полномочий имеют одинаковый формат: переменное количество записей ресурсов, где количество записей указано в соответствующем поле `count` в заголовке.

`SERVER`, `WHEN`, `MSG SIZE`: Отвечающий сервер, время и размер сообщения соответственно.

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

Он будет записан в конце результата команды `"dig"`. Также мы можем использовать команду: `dig itmo.ru +short +identify`, чтобы узнать точный сервер.