DNS - лабораторная работа: dig, часть 1

В следующих лабораторных работах, мы будем использовать "auth1" в качестве
вашей рабочей станции. На самом деле, это не очень важно, потому что
мы будем использовать только лишь команду 'dig'.

DIG
---

1. Выполните DNS-запросы с помощью 'dig':

Замечание: убедитесь, что вы явным образом указываете запрашиваемый
DNS-сервер используя "@":

    $ dig @server_ip ...

Если вы опустите @server_ip, dig будет использовать DNS-сервер(ы), указанные
в /etc/resolv.conf

1a. Выполните каждую команду; смотрите в раздел ответов (ANSWER) и запишите
    результат. Также обратите внимание на значение TTL.

Повторите команду. Изменился ли TTL? Являются ли ответы авторитетными?

	РЕЗУЛЬТАТ 1	РЕЗУЛЬТАТ 2
$ dig @10.20.0.254 your-favorite-domain a		
$ dig @10.20.0.254 www.google.com. a		
$ dig @10.20.0.254 afnog.org. mx		
$ dig @10.20.0.254 NonExistentDomain.sometld any		
$ dig @10.20.0.254 tiscali.co.uk. txt		
$ dig @10.20.0.254 www.afrinic.net aaaa		
$ dig @10.20.0.254 ipv6.google.com aaaa		

1b. Теперь, отправьте запросы другому кэширующему серверу.

    (Выполните каждую из последующих команд дважды, и сравните время выполнения
     (в миллисекундах) каждой попытки)

	РЕЗУЛЬТАТ 1	РЕЗУЛЬТАТ 2
$ dig @8.8.8.8 news.bbc.co.uk. a		
$ dig @208.67.222.222 yahoo.com. a		
$ dig @<a server of your choice> <domain of your choice> a		

    Как долго выполнялись запросы? (В первый раз, и во второй раз)

2. Обратный поиск (по IP)

    Теперь сделайте несколько "обратных" запросов - обратите внимание, что
    мы не указываем явным образом, какой DNS-сервер dig должен запрашивать.
    Какой DNS-сервер будет использован?

    $ dig -x 10.20.X.1
    $ dig -x 10.20.X.2
    $ dig -x 10.20.X.3

    ... где X в диапазоне от 1 до 25

Повторите для любого выбранного вами IP-адреса, в сети Интернет. Помните, что вы должны указывать @10.20.0.254 для того, чтобы осуществлять запросы в Интернет...

Теперь попробуйте запрос:

```
$ dig 1.X.20.10.in-addr.arpa. PTR
```

... ги X в диапазоне от 1 до 25.

На что вы обратили внимание?

Теперь давайте попробуем IPv6:

```
$ dig -x 2001:42d0::200:2:1
```

Какие различия вы наблюдаете между результатами обратных запросов для IPv6 и IPv4-адресов?

Замечание: возможно, вы не получите ответа для IPv6-адреса - тогда сравните раздел запроса для IPv4 и для IPv6.

3. DNSSEC & EDNS0

Попытайтесь выполнить некоторые из предыдущих запросов, добавив опцию "+edns=0".

Например:

```
$ dig @10.20.0.254 www.icann.org +edns=0
```

(возможно, есть смысл использовать команду "more" для ограничения количества выводимой командой информации поэкранно)

```
$ dig @10.20.0.254 www.icann.org +edns=0 | more
```

Обратили внимание на OPT PSEUDOSECTION в начале вывода?

Что интересного вы заметили о подразделе flags: в разделе OPT?

Давайте явным образом включим опцию BUFSIZE, но не EDNS0:

```
$ dig @10.20.0.254 www.icann.org +bufsize=1024 | more
```

Обратите внимание, что EDNS установлен автоматически, и обратите внимание на подраздел udp: size в псевдоразделе OPT.

Теперь, давайте попробуем получить DNSSEC-ответы:

```
$ dig @10.20.0.254 isoc.org DNSKEY | more
$ dig @10.20.0.254 www.isoc.org RRSIG | more
```

Наконец, дадим знать нашему DSN-серверу, что мы поддерживаем DNSSEC:

```
$ dig @10.20.0.254 www.isoc.org A +dnssec
$ dig @10.20.0.254 isoc.org NS +dnssec
```

Обратили ли вы внимание на новое поле в разделе "flags:" ответа?

```
  $ dig @10.20.0.254 www.isoc.org A
  $ dig @10.20.0.254 isoc.org NS
```

Сравните это с выводом dig БЕЗ опции +dnssec:

Если ваша группа уже запустила DNS-сервер, что получится
если вы сделаете DNSSEC-запрос к нему?

```
$ dig @10.20.XXX.3 noc.dns.nsrc.org A +dnssec
$ dig @10.20.XXX.3 dns.nsrc.org NS +dnssec
```

... где XXX - номер вашей группы, и .3 - ваш кэширующий сервер
(но он может быть еще не запущен!)