Week 2

Session 1

Domain Name System

Olga Chernukhina

0. Preparation

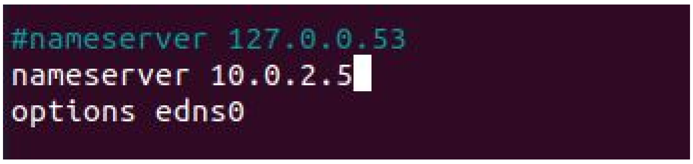
I modified my configuration of the network to the one that was presented to us in the lab and that is more elegantly implemented.

1. BIND9 Caching Only

Install BIND9 and BIND9 tools on one of your clients

In the terminal run `sudo apt-get install bind9 bind9utils bind9-doc`

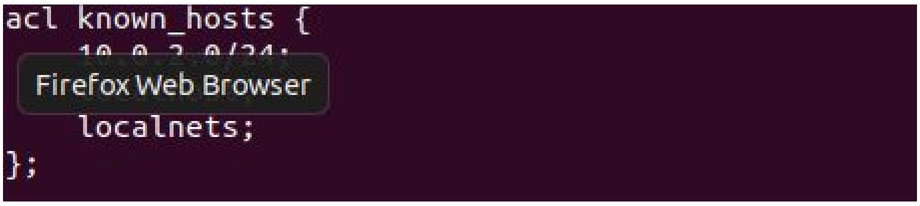
And also on this machine I set nameserver to be the second machine (which is configured as bind9 server):



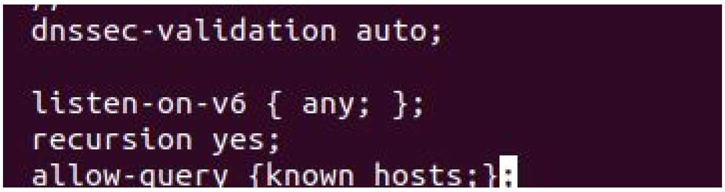
```
#nameserver 127.0.0.53
nameserver 10.0.2.5
options edns0
```

Configure the bind to act as caching only for the other client

I listed localhost, localnets and a subnet of my VMs to have access to bind9:

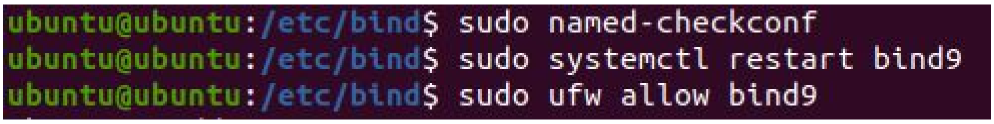


```
acl known_hosts {
    10.0.2.0/24;

    localnets;
};
```



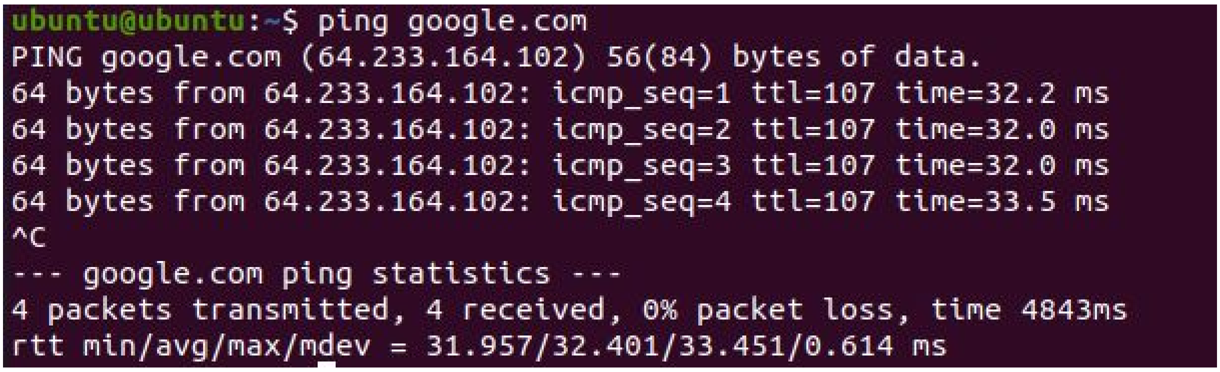
```
 dnssec-validation auto;

 listen-on-v6 { any; };
 recursion yes;
 allow-query {known hosts;};
```

To apply new configuration, allow exception to the firewall policy and check the syntax of our configuration files:



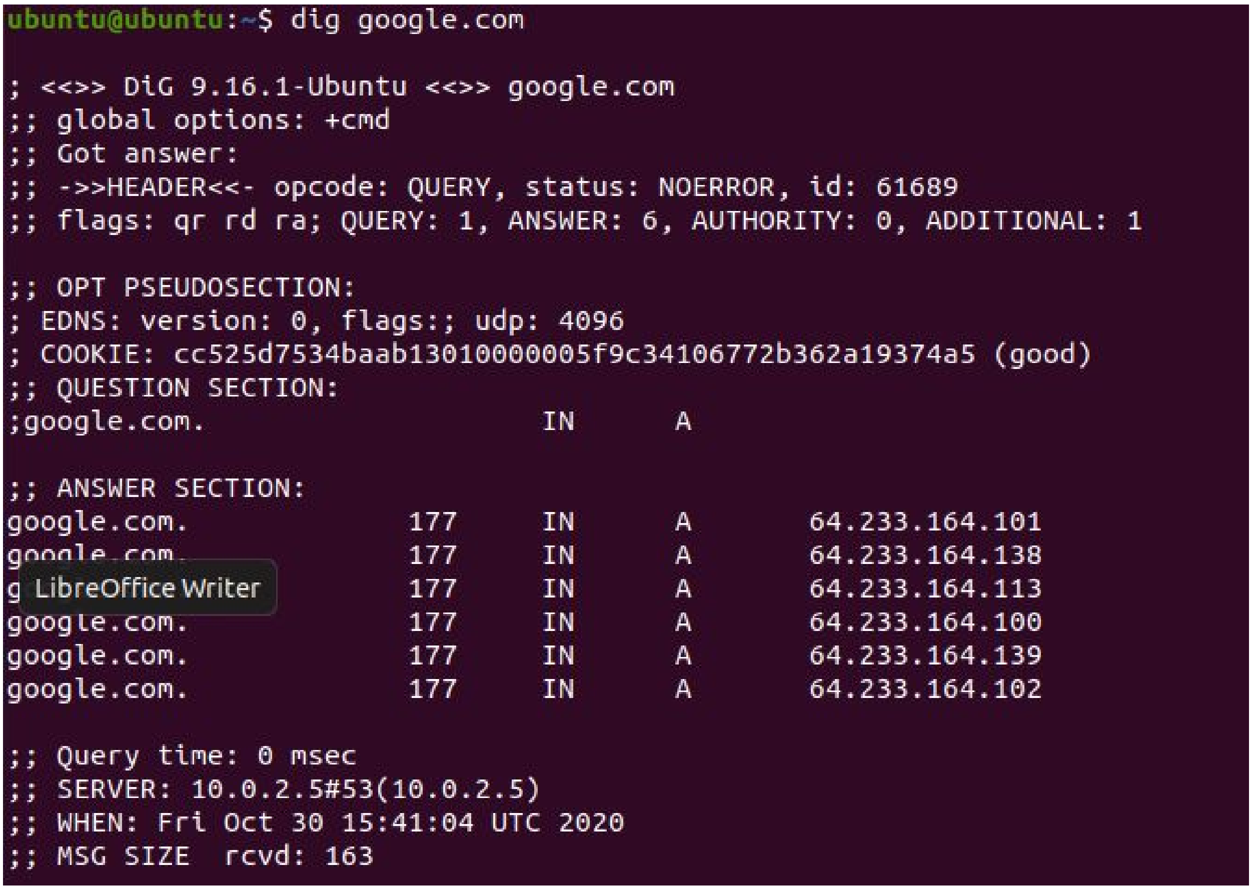
```
ubuntu@ubuntu:/etc/bind$ sudo named-checkconf
ubuntu@ubuntu:/etc/bind$ sudo systemctl restart bind9
ubuntu@ubuntu:/etc/bind$ sudo ufw allow bind9
```

Check if you can access the internet (use ping, dig, nslookup)

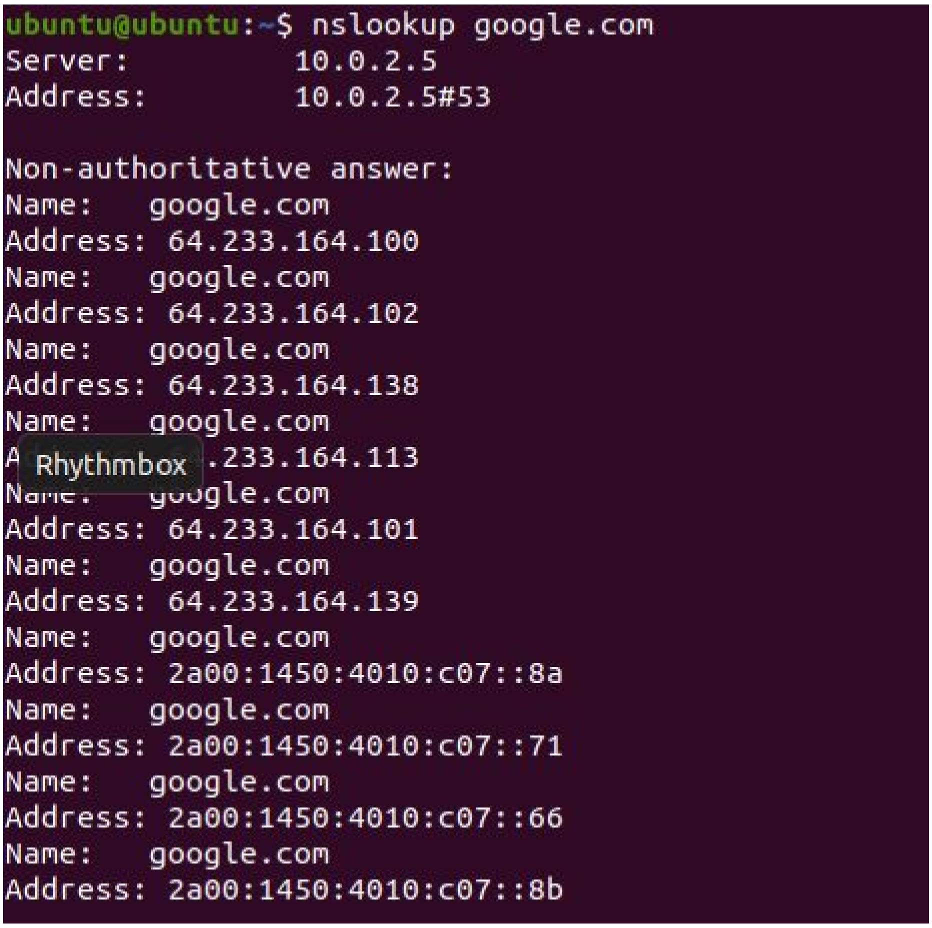


```
ubuntu@ubuntu:~$ ping google.com
PING google.com (64.233.164.102) 56(84) bytes of data.
64 bytes from 64.233.164.102: icmp_seq=1 ttl=107 time=32.2 ms
64 bytes from 64.233.164.102: icmp_seq=2 ttl=107 time=32.0 ms
64 bytes from 64.233.164.102: icmp_seq=3 ttl=107 time=32.0 ms
64 bytes from 64.233.164.102: icmp_seq=4 ttl=107 time=33.5 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 4843ms
rtt min/avg/max/mdev = 31.957/32.401/33.451/0.614 ms
```

Everything works fine :)



```
ubuntu@ubuntu:~$ dig google.com

; <<>> DiG 9.16.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61689
;; flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: cc525d7534baab13010000005f9c34106772b362a19374a5 (good)
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             177     IN      A       64.233.164.101
google.com.             177     IN      A       64.233.164.138
g                       177     IN      A       64.233.164.113
google.com.             177     IN      A       64.233.164.100
google.com.             177     IN      A       64.233.164.139
google.com.             177     IN      A       64.233.164.102

;; Query time: 0 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Fri Oct 30 15:41:04 UTC 2020
;; MSG SIZE  rcvd: 163
```

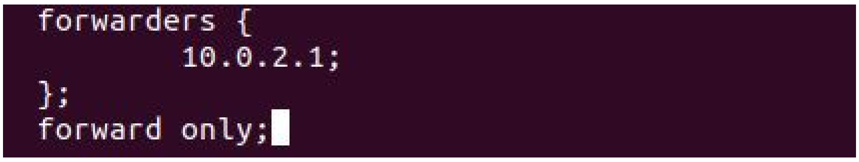


```
ubuntu@ubuntu:~$ nslookup google.com
Server:         10.0.2.5
Address:        10.0.2.5#53

Non-authoritative answer:
Name:   google.com
Address: 64.233.164.100
Name:   google.com
Address: 64.233.164.102
Name:   google.com
Address: 64.233.164.138
Name:   google.com
A Rhythmbox .233.164.113
Name:   google.com
Address: 64.233.164.101
Name:   google.com
Address: 64.233.164.139
Name:   google.com
Address: 2a00:1450:4010:c07::8a
Name:   google.com
Address: 2a00:1450:4010:c07::71
Name:   google.com
Address: 2a00:1450:4010:c07::66
Name:   google.com
Address: 2a00:1450:4010:c07::8b
```

2. BIND9 Caching Only with forwarder

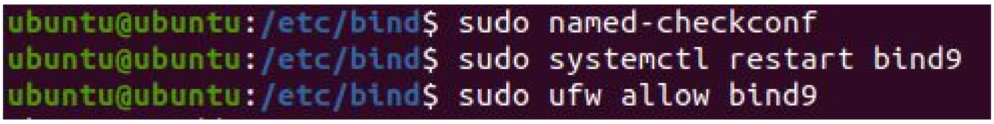
Configure your virtual machine’s NAT Interface (DNS) as forwarder for your first bind9

To add forwarding functionality to the server, list forwarders:



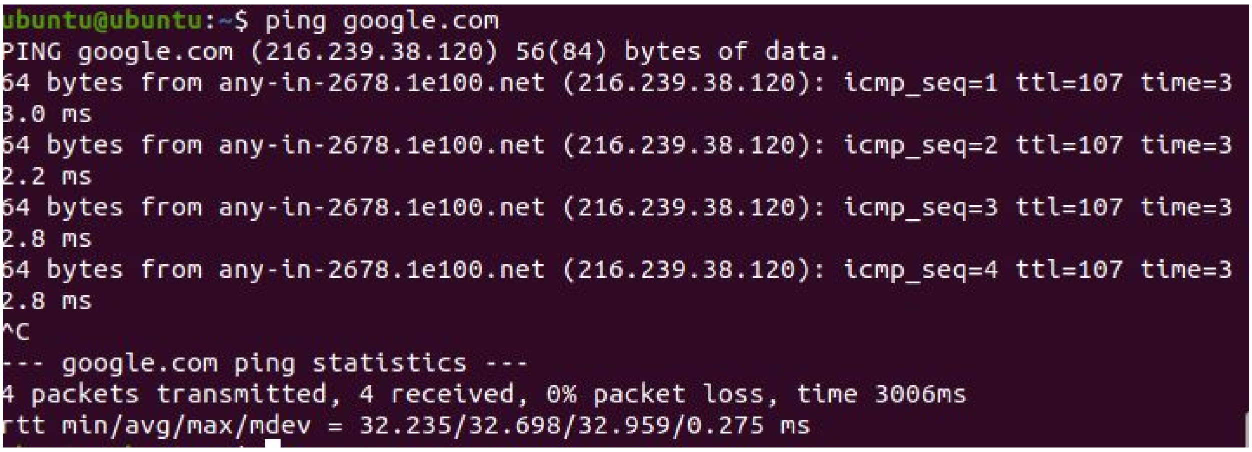
```
 forwarders {
         10.0.2.1;
 };
 forward only;
```

To apply new configuration, allow an exception to the firewall policy and check the syntax of our configuration files:

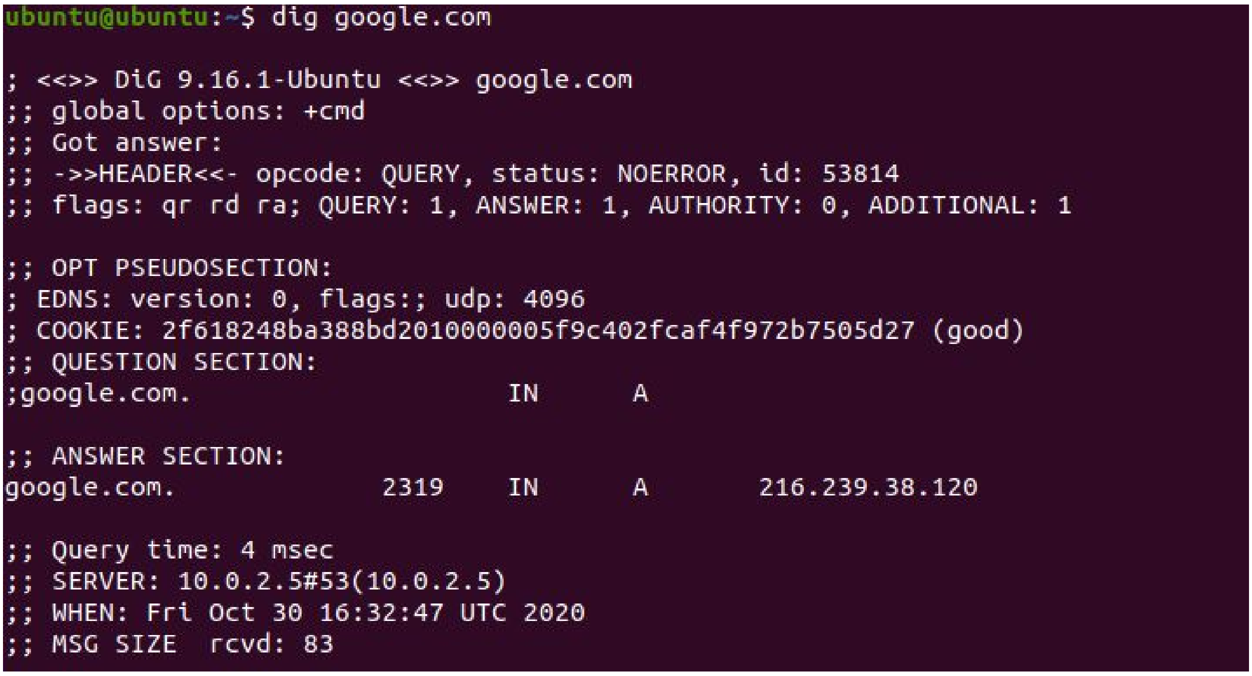


```
ubuntu@ubuntu:/etc/bind$ sudo named-checkconf
ubuntu@ubuntu:/etc/bind$ sudo systemctl restart bind9
ubuntu@ubuntu:/etc/bind$ sudo ufw allow bind9
```

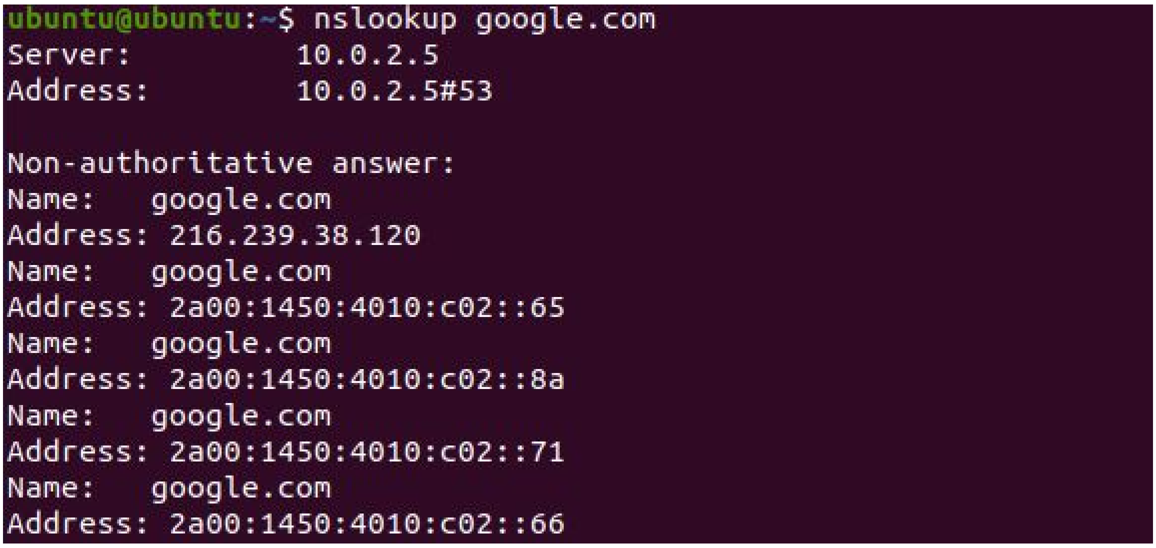
and check the same site again (use ping, dig, nslookup)



```
ubuntu@ubuntu:~$ ping google.com
PING google.com (216.239.38.120) 56(84) bytes of data.
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=1 ttl=107 time=3
3.0 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=2 ttl=107 time=3
2.2 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=3 ttl=107 time=3
2.8 ms
64 bytes from any-in-2678.1e100.net (216.239.38.120): icmp_seq=4 ttl=107 time=3
2.8 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 32.235/32.698/32.959/0.275 ms
```



```
ubuntu@ubuntu:~$ dig google.com

; <<>> DiG 9.16.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53814
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 2f618248ba388bd2010000005f9c402fcaf4f972b7505d27 (good)
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             2319    IN      A       216.239.38.120

;; Query time: 4 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Fri Oct 30 16:32:47 UTC 2020
;; MSG SIZE  rcvd: 83
```

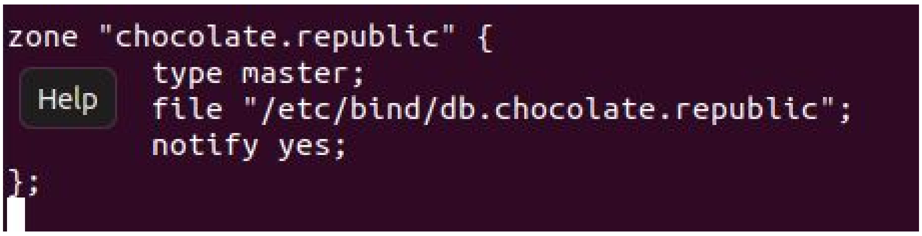


```
ubuntu@ubuntu:~$ nslookup google.com
Server:         10.0.2.5
Address:        10.0.2.5#53

Non-authoritative answer:
Name:   google.com
Address: 216.239.38.120
Name:   google.com
Address: 2a00:1450:4010:c02::65
Name:   google.com
Address: 2a00:1450:4010:c02::8a
Name:   google.com
Address: 2a00:1450:4010:c02::71
Name:   google.com
Address: 2a00:1450:4010:c02::66
```

3. BIND9 Master Authoritative

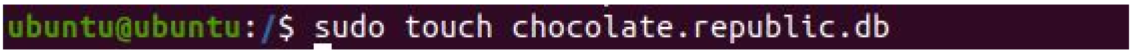
Create a forward lookup zone in your first bind9 and then create `A`, `AAAA`, `NS`, `TXT`, `CNAME` records in it.

Create a new zone in `/etc/bind/named.conf.default-zones`:



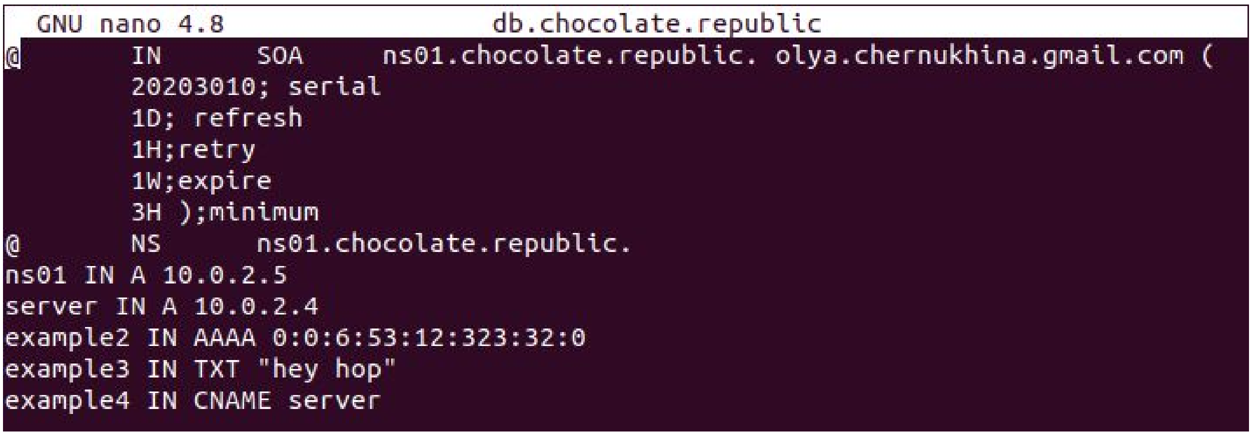
```
zone "chocolate.republic" {
         type master;
         file "/etc/bind/db.chocolate.republic";
         notify yes;
};
```

Also create a file for this zone:



```
ubuntu@ubuntu:/$ sudo touch chocolate.republic.db
```

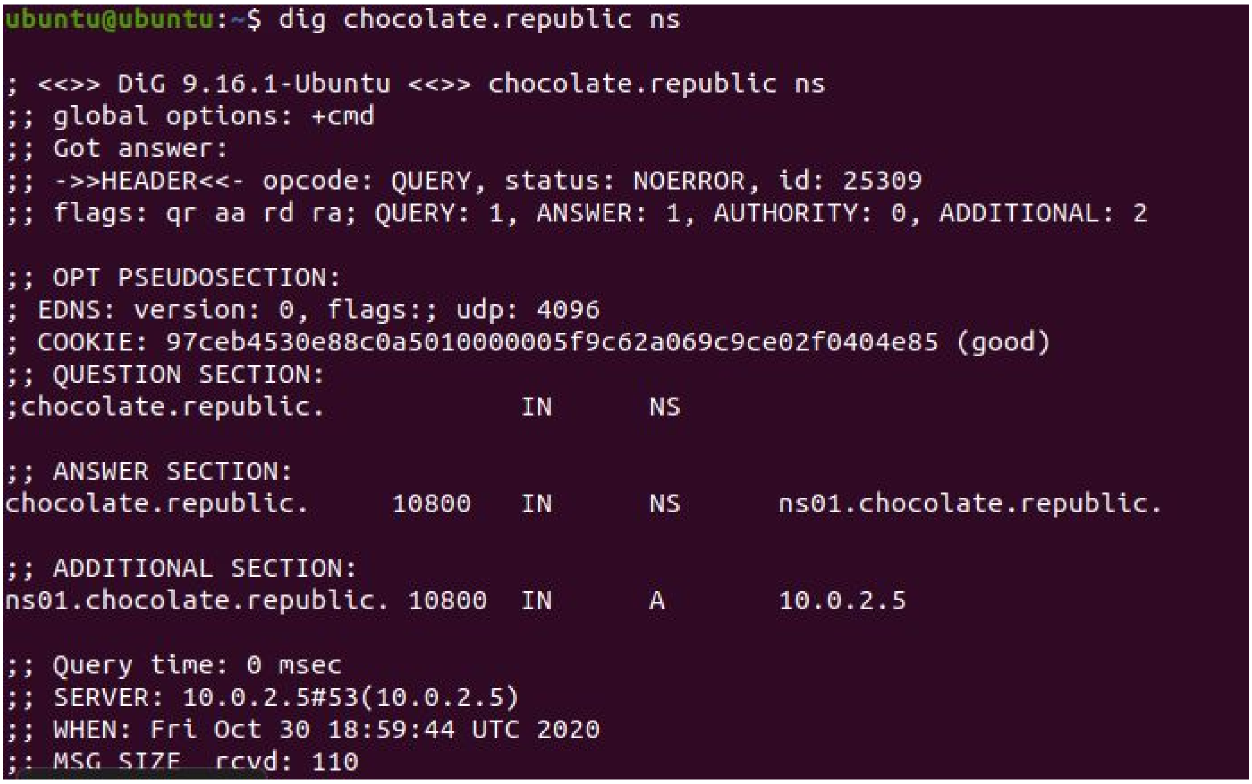
Add some DNS record of different types:



```
  GNU nano 4.8                    db.chocolate.republic
@       IN      SOA     ns01.chocolate.republic. olya.chernukhina.gmail.com (
        20203010; serial
        1D; refresh
        1H;retry
        1W;expire
        3H );minimum
@       NS      ns01.chocolate.republic.
ns01 IN A 10.0.2.5
server IN A 10.0.2.4
example2 IN AAAA 0:0:6:53:12:323:32:0
example3 IN TXT "hey hop"
example4 IN CNAME server
```

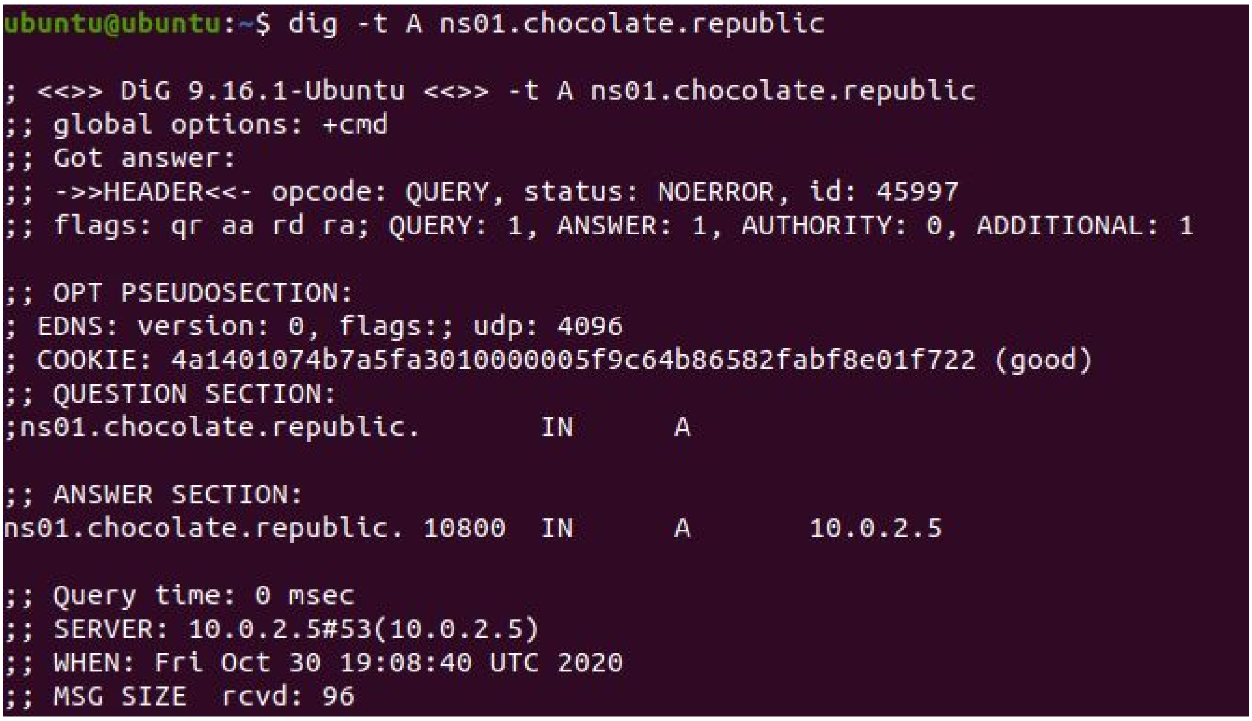
Verify your records from other machine using ping, dig and nslookup.

Type NS:

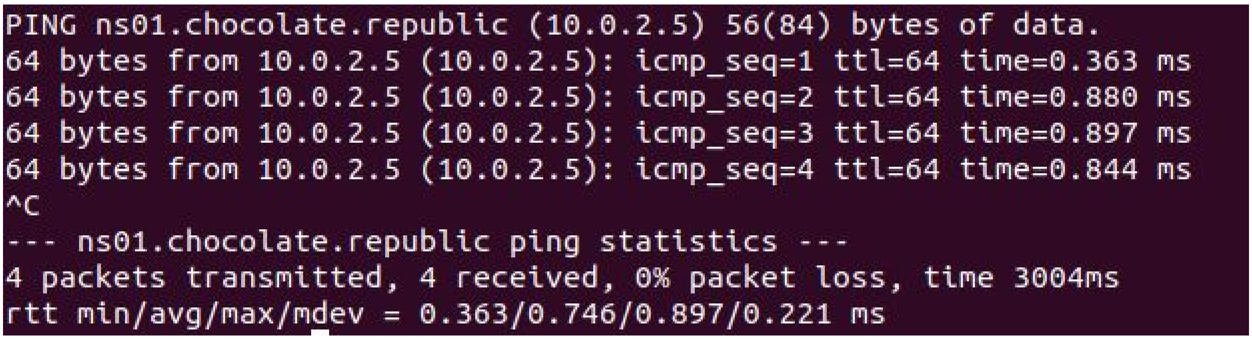


```
ubuntu@ubuntu:~$ dig chocolate.republic ns

; <<>> DiG 9.16.1-Ubuntu <<>> chocolate.republic ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25309
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 97ceb4530e88c0a5010000005f9c62a069c9ce02f0404e85 (good)
;; QUESTION SECTION:
;chocolate.republic.            IN      NS

;; ANSWER SECTION:
chocolate.republic.     10800   IN      NS      ns01.chocolate.republic.

;; ADDITIONAL SECTION:
ns01.chocolate.republic. 10800  IN      A       10.0.2.5

;; Query time: 0 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Fri Oct 30 18:59:44 UTC 2020
;; MSG SIZE  rcvd: 110
```

Type A:

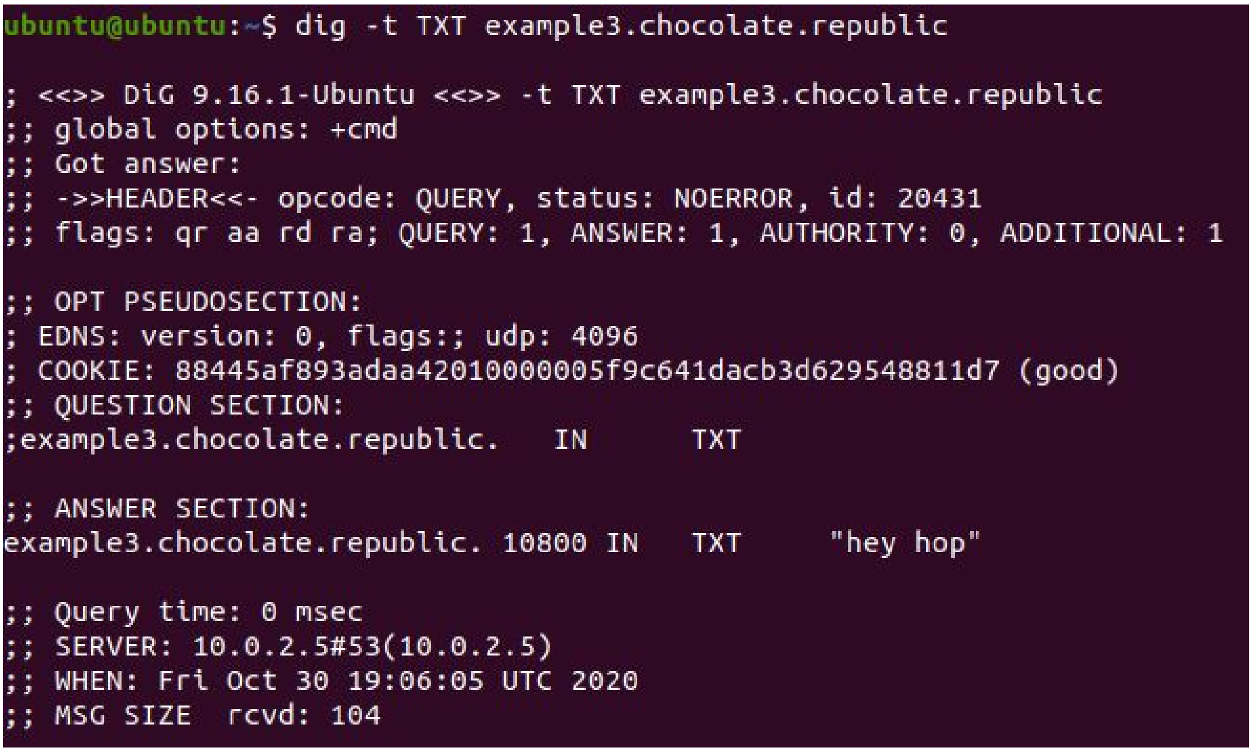


```
ubuntu@ubuntu:~$ dig -t A ns01.chocolate.republic

; <<>> DiG 9.16.1-Ubuntu <<>> -t A ns01.chocolate.republic
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45997
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 4a1401074b7a5fa3010000005f9c64b86582fabf8e01f722 (good)
;; QUESTION SECTION:
;ns01.chocolate.republic.       IN      A

;; ANSWER SECTION:
ns01.chocolate.republic. 10800  IN      A       10.0.2.5

;; Query time: 0 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Fri Oct 30 19:08:40 UTC 2020
;; MSG SIZE  rcvd: 96
```



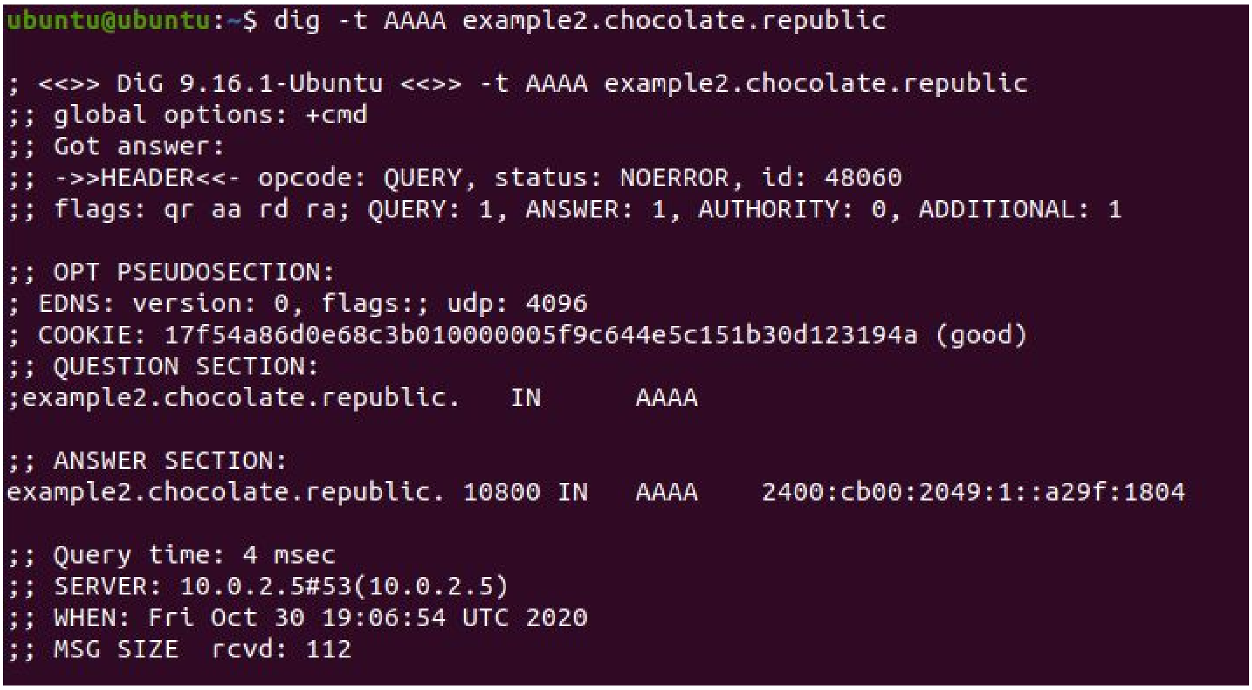
```
PING ns01.chocolate.republic (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5 (10.0.2.5): icmp_seq=1 ttl=64 time=0.363 ms
64 bytes from 10.0.2.5 (10.0.2.5): icmp_seq=2 ttl=64 time=0.880 ms
64 bytes from 10.0.2.5 (10.0.2.5): icmp_seq=3 ttl=64 time=0.897 ms
64 bytes from 10.0.2.5 (10.0.2.5): icmp_seq=4 ttl=64 time=0.844 ms
^C
--- ns01.chocolate.republic ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.363/0.746/0.897/0.221 ms
```

Type TXT:



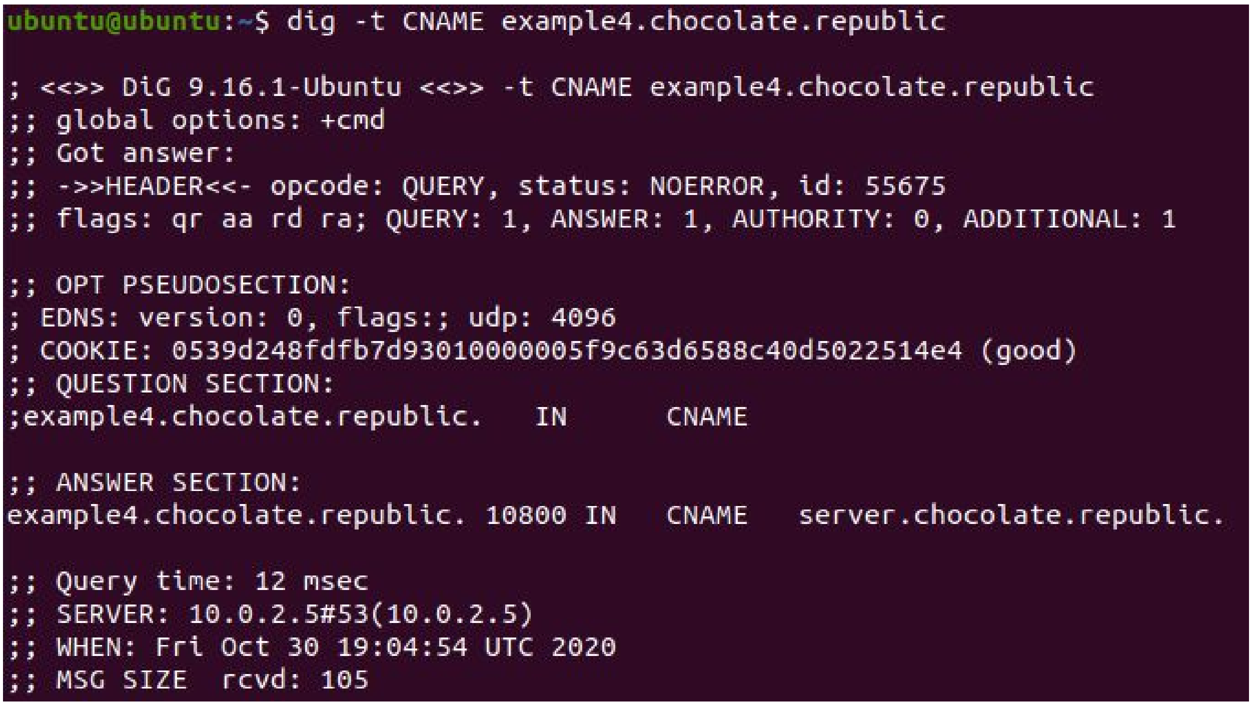
```
ubuntu@ubuntu:~$ dig -t TXT example3.chocolate.republic

; <<>> DiG 9.16.1-Ubuntu <<>> -t TXT example3.chocolate.republic
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20431
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 88445af893adaa42010000005f9c641dacb3d629548811d7 (good)
;; QUESTION SECTION:
;example3.chocolate.republic.   IN      TXT

;; ANSWER SECTION:
example3.chocolate.republic. 10800 IN   TXT     "hey hop"

;; Query time: 0 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Fri Oct 30 19:06:05 UTC 2020
;; MSG SIZE  rcvd: 104
```

Type AAAA:

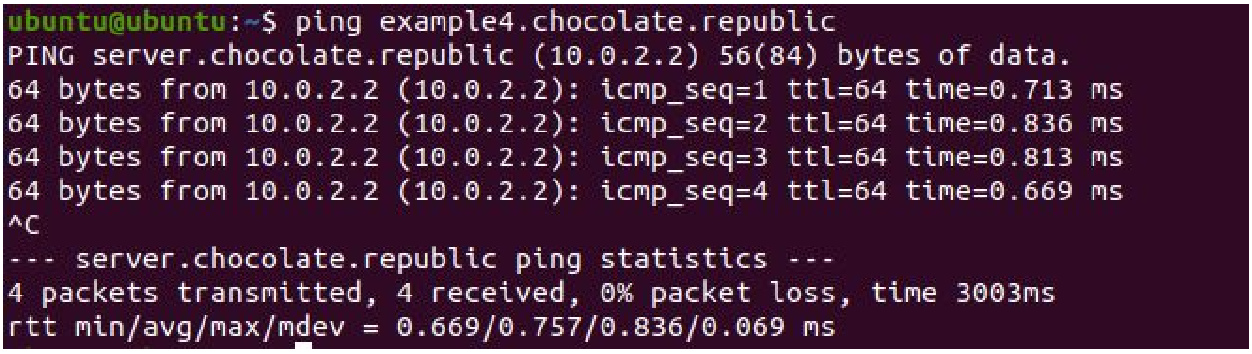


```
ubuntu@ubuntu:~$ dig -t AAAA example2.chocolate.republic

; <<>> DiG 9.16.1-Ubuntu <<>> -t AAAA example2.chocolate.republic
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48060
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 17f54a86d0e68c3b010000005f9c644e5c151b30d123194a (good)
;; QUESTION SECTION:
;example2.chocolate.republic.   IN      AAAA

;; ANSWER SECTION:
example2.chocolate.republic. 10800 IN   AAAA    2400:cb00:2049:1::a29f:1804

;; Query time: 4 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Fri Oct 30 19:06:54 UTC 2020
;; MSG SIZE  rcvd: 112
```

Type CNAME:



```
ubuntu@ubuntu:~$ dig -t CNAME example4.chocolate.republic

; <<>> DiG 9.16.1-Ubuntu <<>> -t CNAME example4.chocolate.republic
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55675
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 0539d248fdfb7d93010000005f9c63d6588c40d5022514e4 (good)
;; QUESTION SECTION:
;example4.chocolate.republic.   IN      CNAME

;; ANSWER SECTION:
example4.chocolate.republic. 10800 IN   CNAME   server.chocolate.republic.

;; Query time: 12 msec
;; SERVER: 10.0.2.5#53(10.0.2.5)
;; WHEN: Fri Oct 30 19:04:54 UTC 2020
;; MSG SIZE  rcvd: 105
```

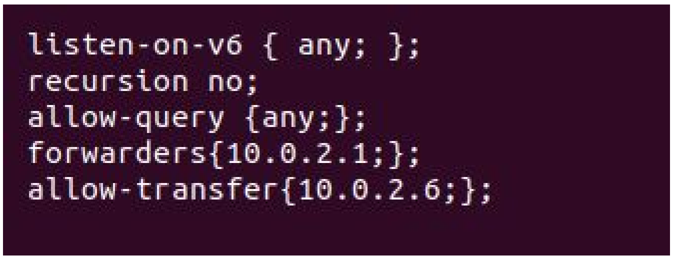


```
ubuntu@ubuntu:~$ ping example4.chocolate.republic
PING server.chocolate.republic (10.0.2.2) 56(84) bytes of data.
64 bytes from 10.0.2.2 (10.0.2.2): icmp_seq=1 ttl=64 time=0.713 ms
64 bytes from 10.0.2.2 (10.0.2.2): icmp_seq=2 ttl=64 time=0.836 ms
64 bytes from 10.0.2.2 (10.0.2.2): icmp_seq=3 ttl=64 time=0.813 ms
64 bytes from 10.0.2.2 (10.0.2.2): icmp_seq=4 ttl=64 time=0.669 ms
^C
--- server.chocolate.republic ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.669/0.757/0.836/0.069 ms
```

4. BIND9 Slave

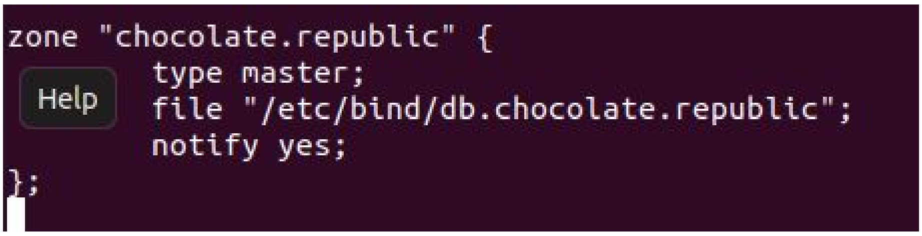
Install bind9 on your second vm and configure your servervm or your desktop to use the second vm as DNS server

Add allow-transfer file to the `/etc/bind/named.conf.options` on master



```
listen-on-v6 { any; };
recursion no;
allow-query {any;};
forwarders{10.0.2.1;};
allow-transfer{10.0.2.6;};
```

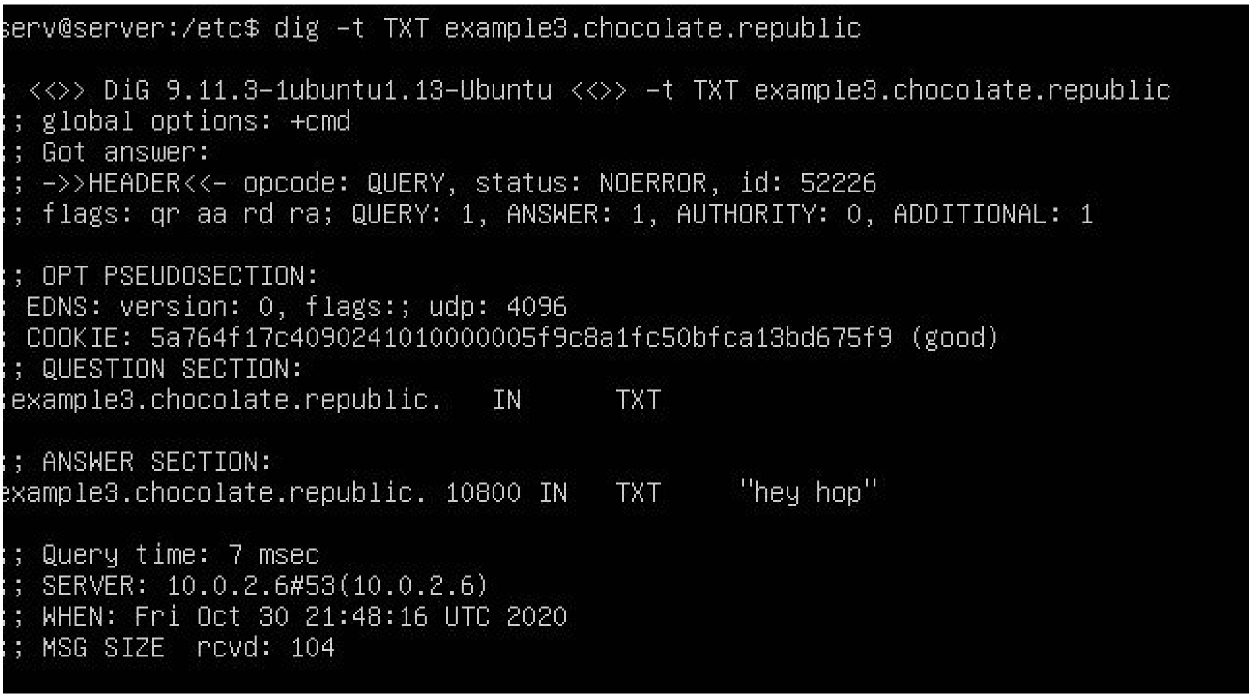
Add a new zone in /etc/bind/named.conf.default-zones on slave



```
zone "chocolate.republic" {
        type master;
        file "/etc/bind/db.chocolate.republic";
        notify yes;
};
```

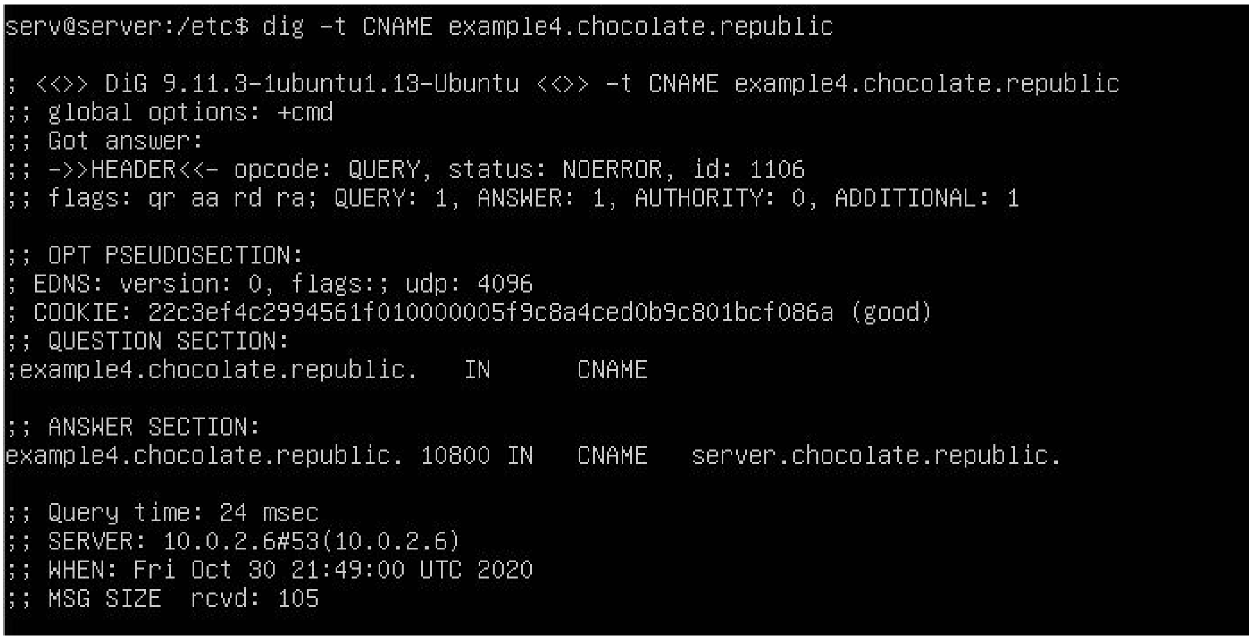
Check for the records that you created on first bind9 using mentioned tools.

Type NS:



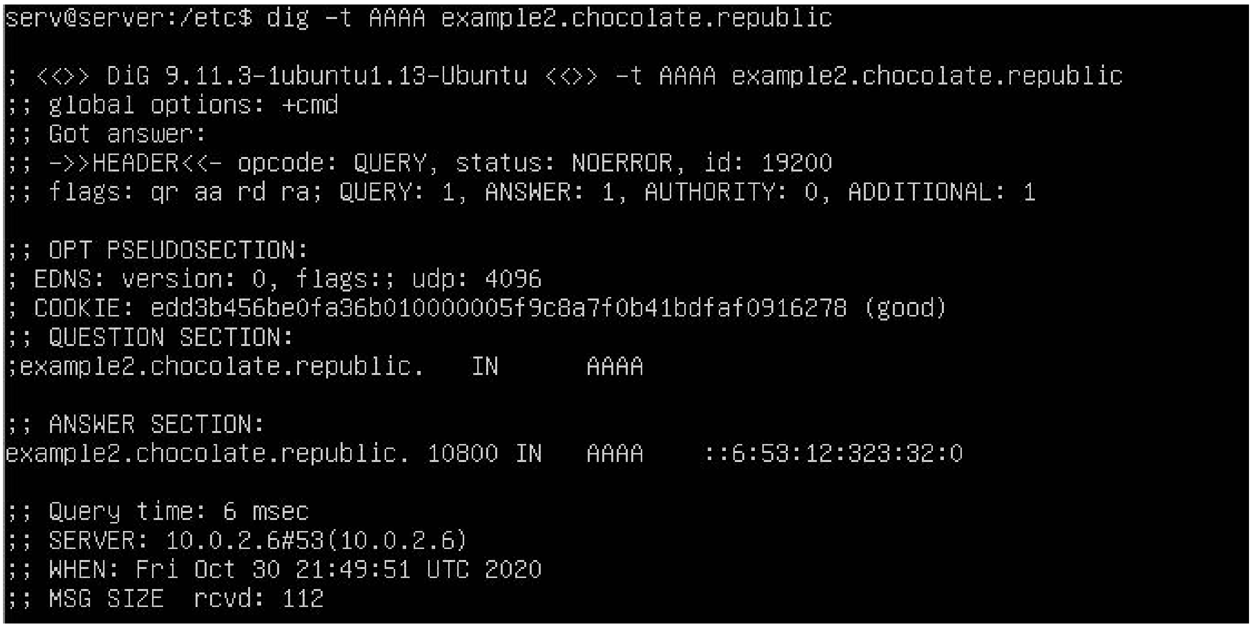
```
serv@server:/etc$ dig -t TXT example3.chocolate.republic

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> -t TXT example3.chocolate.republic
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52226
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 5a764f17c40902410100000005f9c8a1fc50bfca13bd675f9 (good)
;; QUESTION SECTION:
;example3.chocolate.republic.   IN      TXT

;; ANSWER SECTION:
example3.chocolate.republic. 10800 IN   TXT     "hey hop"

;; Query time: 7 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Oct 30 21:48:16 UTC 2020
;; MSG SIZE  rcvd: 104
```

Type CNAME:



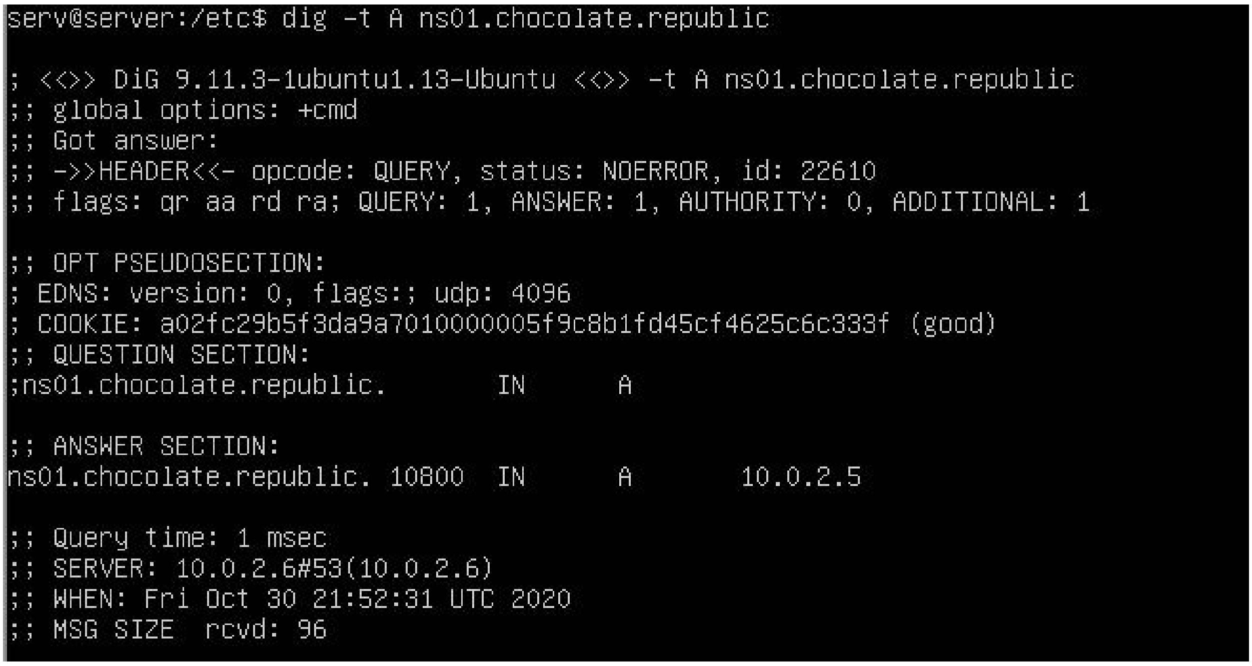
```
serv@server:/etc$ dig -t CNAME example4.chocolate.republic

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> -t CNAME example4.chocolate.republic
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1106
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 22c3ef4c2994561f010000005f9c8a4ced0b9c801bcf086a (good)
;; QUESTION SECTION:
;example4.chocolate.republic.   IN      CNAME

;; ANSWER SECTION:
example4.chocolate.republic. 10800 IN   CNAME   server.chocolate.republic.

;; Query time: 24 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Oct 30 21:49:00 UTC 2020
;; MSG SIZE  rcvd: 105
```

Type AAAA:



```
serv@server:/etc$ dig -t AAAA example2.chocolate.republic

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> -t AAAA example2.chocolate.republic
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19200
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: edd3b456be0fa36b010000005f9c8a7f0b41bdfaf0916278 (good)
;; QUESTION SECTION:
;example2.chocolate.republic.   IN      AAAA

;; ANSWER SECTION:
example2.chocolate.republic. 10800 IN   AAAA    ::6:53:12:323:32:0

;; Query time: 6 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Oct 30 21:49:51 UTC 2020
;; MSG SIZE  rcvd: 112
```

Type A:



```
serv@server:/etc$ dig -t A ns01.chocolate.republic

; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> -t A ns01.chocolate.republic
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22610
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: a02fc29b5f3da9a7010000005f9c8b1fd45cf4625c6c333f (good)
;; QUESTION SECTION:
;ns01.chocolate.republic.       IN      A

;; ANSWER SECTION:
ns01.chocolate.republic. 10800  IN      A       10.0.2.5

;; Query time: 1 msec
;; SERVER: 10.0.2.6#53(10.0.2.6)
;; WHEN: Fri Oct 30 21:52:31 UTC 2020
;; MSG SIZE  rcvd: 96
```

Note - the Server IP has changed, hence, the records appeared on the second server

5. Bonus

What is fierce.pl?

Fierce.pl it is specifically designed to identify potential targets within and outside of your company's network. This script quickly scans areas using multiple tactics (usually only within minutes if there is no network delay).

Firstly, it queries DNS destinations for DNS servers. What then takes turn is to use the target DNS server (optional, you can use another one using the dns server switch). Then try to reset the domain's SOA records in hopes that the DNS server target is using may be incorrectly configured.

If it does not succeed (as it almost always is), it will try to "guess" the common name of many different companies.

What is DNS hijacking?

It is hacking the DNS service from an Internet service provider and changing some addresses. When a user tries to connect to a site which address was changed by attackers, they are actually redirected to a specially constructed so-called fishing site. This fake site looks exactly the same as the real one, but when the user logs in, nothing happens. In fact, the site records the user's registration data, so hackers can use them to connect to the real site.

Sources:
https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-caching-or-forwarding-dns-server-on-ubuntu-16-04

https://www.dedoimedo.com/computers/virtualbox-nat-networks.html

https://www.serverlab.ca/tutorials/linux/network-services/how-to-create-forward-lookup-zones-for-bind/

http://dedicatesupport.com/content/bind9-rezhim-masterslave