

# Domain Name System

## Enterprise Digital Infrastructure – Assignment #2

This is a series of screenshots and commands in bash used to answer all questions. This is a "support" PDF to the main project report, in which there are no screenshots and it is shorter.

### Active Experiments:

The *name server* by default, in the */etc/resolv.conf* file is: 127.0.0.53

To change the name server, edit the file above. Change it with the IP address (8.8.8.8) of the Google public name server. The same experiments are performed using Cloudflare's public DNS name server (1.1.1.1) to see if there are any differences.

### Question 1

*dig ercole.unipv.it*  
*dig @1.1.1.1 ercole.unipv.it*

```
davide@davide-hp:~$ dig ercole.unipv.it

;<<> DiG 9.16.1-Ubuntu <<> ercole.unipv.it
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 889
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 1220
;; COOKIE: 8765d68137415f6614bd568a6269771d838529f3dd7647ee (good)
;; QUESTION SECTION:
;ercole.unipv.it.      IN      A

;; ANSWER SECTION:
ercole.unipv.it.      300     IN      A      193.204.34.13

;; Query time: 20 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: mer apr 27 19:02:21 CEST 2022
;; MSG SIZE rcvd: 88
```

```
davide@davide-hp:~$ dig @1.1.1.1 ercole.unipv.it

;<<> DiG 9.16.1-Ubuntu <<> @1.1.1.1 ercole.unipv.it
;; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 20466
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 4096
;; QUESTION SECTION:
;ercole.unipv.it.      IN      A

;; ANSWER SECTION:
ercole.unipv.it.      277     IN      A      193.204.34.13

;; Query time: 0 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: mer apr 27 19:02:44 CEST 2022
;; MSG SIZE rcvd: 60
```

*dig www.sicurezza nazionale.gov.it*  
*dig @1.1.1.1 www.sicurezza nazionale.gov.it*

```
davide@davide-hp:~$ dig www.sicurezza nazionale.gov.it

;<<> DiG 9.16.1-Ubuntu <<> www.sicurezza nazionale.gov.it
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 13982
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 4096
;; QUESTION SECTION:
;www.sicurezza nazionale.gov.it. IN      A

;; ANSWER SECTION:
www.sicurezza nazionale.gov.it. 2395 IN  A      151.13.11.188

;; Query time: 4 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: mer apr 27 19:03:16 CEST 2022
;; MSG SIZE rcvd: 74
```

```
davide@davide-hp:~$ dig @1.1.1.1 www.sicurezza nazionale.gov.it

;<<> DiG 9.16.1-Ubuntu <<> @1.1.1.1 www.sicurezza nazionale.gov.it
;; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 33791
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 4096
;; QUESTION SECTION:
;www.sicurezza nazionale.gov.it. IN      A

;; ANSWER SECTION:
www.sicurezza nazionale.gov.it. 2365 IN  A      151.13.11.188

;; Query time: 4 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: mer apr 27 19:03:46 CEST 2022
;; MSG SIZE rcvd: 74
```

The answers are not authoritative, because they do not come from the authoritative name server of the targets and in fact, as you can see from the photos in the *flags* section, there is no abbreviation aa.

## Question 2

*dig berkeley.edu -t MX*  
*dig @1.1.1.1 berkeley.edu -t MX*

```
davide@davide-hp:~$ dig berkeley.edu -t MX
;<<<> DiG 9.16.1-Ubuntu <<<> berkeley.edu -t MX
;; global options: +cmd
;; Got answer:
;; -->HEADER<<-- opcode: QUERY, status: NOERROR, id: 44368
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
; berkeley.edu.
; IN MX
;; ANSWER SECTION:
berkeley.edu. 2 IN MX 1 aspmx.l.google.com.
berkeley.edu. 2 IN MX 5 alt2.aspmx.l.google.com.
berkeley.edu. 2 IN MX 5 alt1.aspmx.l.google.com.
berkeley.edu. 2 IN MX 10 alt3.aspmx.l.google.com.
berkeley.edu. 2 IN MX 10 alt4.aspmx.l.google.com.
; Query time: 52 msec
; SERVER: 8.8.8.8#53(8.8.8.8)
; WHEN: sab apr 30 14:19:43 CEST 2022
; MSG SIZE rcvd: 159

davide@davide-hp:~$ dig @1.1.1.1 berkeley.edu -t MX
;<<<> DiG 9.16.1-Ubuntu <<<> @1.1.1.1 berkeley.edu -t MX
;; 1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<<-- opcode: QUERY, status: NOERROR, id: 18485
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; DNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
; berkeley.edu.
; IN MX
;; ANSWER SECTION:
berkeley.edu. 70 IN MX 1 aspmx.l.google.com.
berkeley.edu. 70 IN MX 5 alt1.aspmx.l.google.com.
berkeley.edu. 70 IN MX 5 alt2.aspmx.l.google.com.
berkeley.edu. 70 IN MX 10 alt3.aspmx.l.google.com.
berkeley.edu. 70 IN MX 10 alt4.aspmx.l.google.com.
; Query time: 40 msec
; SERVER: 1.1.1.1#53(1.1.1.1)
; WHEN: sab apr 30 14:20:43 CEST 2022
; MSG SIZE rcvd: 159
```

*dig universitadipavia.it -t MX*  
*dig @1.1.1.1 universitadipavia.it -t MX*

```
davide@davide-hp:~$ dig universitadipavia.it -t MX
;<<<> DiG 9.16.1-Ubuntu <<<> universitadipavia.it -t MX
;; global options: +cmd
;; Got answer:
;; -->HEADER<<-- opcode: QUERY, status: NOERROR, id: 4305
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1220
;; COOKIE: 7dc91806bcac227873ed70f062697864d2a3ae5a6c11a192 (good)
;; QUESTION SECTION:
; universitadipavia.it.
; IN MX
;; ANSWER SECTION:
universitadipavia.it. 3600 IN MX 10 ASPMX5.GOOGLEMAIL.COM.
universitadipavia.it. 3600 IN MX 10 ASPMX3.GOOGLEMAIL.COM.
universitadipavia.it. 3600 IN MX 10 ASPMX4.GOOGLEMAIL.COM.
universitadipavia.it. 3600 IN MX 5 ALT1.ASPMX.L.GOOGLE.COM.
universitadipavia.it. 3600 IN MX 10 ASPMX2.GOOGLEMAIL.COM.
universitadipavia.it. 3600 IN MX 5 ALT2.ASPMX.L.GOOGLE.COM.
universitadipavia.it. 3600 IN MX 1 ASPMX.L.GOOGLE.COM.
; Query time: 24 msec
; SERVER: 8.8.8.8#53(8.8.8.8)
; WHEN: mer apr 27 19:07:48 CEST 2022
; MSG SIZE rcvd: 256

davide@davide-hp:~$ dig @1.1.1.1 universitadipavia.it -t MX
;<<<> DiG 9.16.1-Ubuntu <<<> @1.1.1.1 universitadipavia.it -t MX
;; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<<-- opcode: QUERY, status: NOERROR, id: 45412
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1220
;; COOKIE: bb9f71b8429d05c1c7ae7e8d6269787994cac697dc555d7f (good)
;; QUESTION SECTION:
; universitadipavia.it.
; IN MX
;; ANSWER SECTION:
universitadipavia.it. 3600 IN MX 1 ASPMX.L.GOOGLE.COM.
universitadipavia.it. 3600 IN MX 10 ASPMX3.GOOGLEMAIL.COM.
universitadipavia.it. 3600 IN MX 10 ASPMX4.GOOGLEMAIL.COM.
universitadipavia.it. 3600 IN MX 5 ALT1.ASPMX.L.GOOGLE.COM.
universitadipavia.it. 3600 IN MX 10 ASPMX2.GOOGLEMAIL.COM.
universitadipavia.it. 3600 IN MX 10 ASPMX5.GOOGLEMAIL.COM.
; Query time: 20 msec
; SERVER: 1.1.1.1#53(1.1.1.1)
; WHEN: mer apr 27 19:08:09 CEST 2022
; MSG SIZE rcvd: 256
```

There are **five** servers that provide the mail service for *berkeley.edu*, while there are **seven** servers for *universitadipavia.it*. The servers used by the two universities are made available by Google and some of these (ALT1.ASPMX.L.GOOGLE.COM. - ALT2.ASPMX.L.GOOGLE.COM. - ASPMX.L.GOOGLE.COM.) are shared for the two universities. In fact, even checking with the *ping* / *dig* commands shows that the IP addresses match. Also note that the *berkeley.edu* domain uses DNSSEC to sign records.

## Question 3

*dig www.japan.go.jp*  
*dig @1.1.1.1 www.japan.go.jp*

The answers are not authoritative, because they do not come from the authoritative name server of the [Government of Japan](#) domain and in fact, as you can see from the photos in the *flags* section, there is no abbreviation aa. **Four** RRs are obtained: all of type A.

```
davide@davide-hp:~$ dig www.japan.go.jp

;<<> DiG 9.16.1-Ubuntu <<> www.japan.go.jp
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 7220
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 512
;; QUESTION SECTION:
;www.japan.go.jp.                IN      A

;; ANSWER SECTION:
www.japan.go.jp.        60      IN      A      99.86.153.83
www.japan.go.jp.        60      IN      A      99.86.153.69
www.japan.go.jp.        60      IN      A      99.86.153.84
www.japan.go.jp.        60      IN      A      99.86.153.30

;; Query time: 55 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: sab apr 30 17:19:11 CEST 2022
;; MSG SIZE rcvd: 108
```

```
davide@davide-hp:~$ dig @1.1.1.1 www.japan.go.jp

;<<> DiG 9.16.1-Ubuntu <<> @1.1.1.1 www.japan.go.jp
;; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 15490
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 1232
;; QUESTION SECTION:
;www.japan.go.jp.                IN      A

;; ANSWER SECTION:
www.japan.go.jp.        60      IN      A      99.86.153.30
www.japan.go.jp.        60      IN      A      99.86.153.69
www.japan.go.jp.        60      IN      A      99.86.153.83
www.japan.go.jp.        60      IN      A      99.86.153.84

;; Query time: 555 msec
;; SERVER: 1.1.1.1#53(1.1.1.1)
;; WHEN: sab apr 30 17:19:43 CEST 2022
;; MSG SIZE rcvd: 108
```

*dig www.japan.go.jp +dnssec*  
*whois www.japan.go.jp*

```
davide@davide-hp:~$ dig www.japan.go.jp +dnssec

;<<> DiG 9.16.1-Ubuntu <<> www.japan.go.jp +dnssec
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 62302
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: do; udp: 512
;; QUESTION SECTION:
;www.japan.go.jp.                IN      A

;; ANSWER SECTION:
www.japan.go.jp.        60      IN      A      99.86.153.83
www.japan.go.jp.        60      IN      A      99.86.153.30
www.japan.go.jp.        60      IN      A      99.86.153.84
www.japan.go.jp.        60      IN      A      99.86.153.69
www.japan.go.jp.        60      IN      RRSIG  A 13 4 60 20220430162259 20220430142159 20602 japan.go.jp. HIKS+wcaYBxuzt57NEHLVzH5wJzAcmWycvUT9afNUzZ5tL5drLYqrZUM GwLxFn10t8W/+H1z2L0+UCKW
jfwg==

;; Query time: 43 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: sab apr 30 17:21:59 CEST 2022
;; MSG SIZE rcvd: 215
```

```
davide@davide-hp:~$ whois japan.go.jp
[ JPRS database provides information on network administration. Its use is
[ restricted to network administration purposes. For further information,
[ use 'whois -h whois.jprs.jp help'. To suppress Japanese output, add'/e'
[ at the end of command, e.g. 'whois -h whois.jprs.jp xxx/e'.
[

Domain Information:
a. [Domain Name]                JAPAN.GO.JP
g. [Organization]              Public Relations Office, Cabinet Office, Government of Japan
l. [Organization Type]         Government
m. [Administrative Contact]    T043364JP
n. [Technical Contact]        HS58433JP
p. [Name Server]              ns-360.awsdns-45.com
p. [Name Server]              ns-1100.awsdns-09.org
p. [Name Server]              ns-1588.awsdns-06.co.uk
p. [Name Server]              ns-688.awsdns-21.net
s. [Signing Key]              19228 13 2 (
                               6F85762A890865AF4B510AB5BB3EECA6
                               961FF7524CB866A3860A60D138B0C395 )

[State]                        Connected (2022/04/30)
[Registered Date]              2014/04/22
[Connected Date]               2014/05/22
[Last Update]                  2021/09/19 01:52:48 (JST)
```

Querying through dig, adding the flag `+dnssec` it results that the domain uses DNSSEC. Also with the `whois` command shows that the DNSSEC signature field is not empty.

## Question 4

`dig dell.com -t NS`  
`dig @1.1.1.1 dell.com -t NS`

```
davide@davide-hp:~$ dig dell.com -t NS

> DiG 9.16.1-Ubuntu <<>> dell.com -t NS
Global options: +cmd
Got answer:
->HEADER<- opcode: QUERY, status: NOERROR, id: 14558
Flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

OPT PSEUDOSECTION:
DNS: version: 0, flags:; udp: 512
QUESTION SECTION:
dell.com.                IN      NS

ANSWER SECTION:
dell.com.                600     IN      NS      ns5.us.dell.com.
dell.com.                600     IN      NS      ns4.us.dell.com.
dell.com.                600     IN      NS      ns3.us.dell.com.
dell.com.                600     IN      NS      ns6.us.dell.com.
dell.com.                600     IN      NS      ns1.us.dell.com.
dell.com.                600     IN      NS      ns2.us.dell.com.

SERVER: 8.8.8.8#53(8.8.8.8)
When: sab apr 30 17:27:48 CEST 2022
MSG SIZE rcvd: 148
```

```
davide@davide-hp:~$ dig @1.1.1.1 dell.com -t NS

>>> DiG 9.16.1-Ubuntu <<>> @1.1.1.1 dell.com -t NS
(server found)
Global options: +cmd
Got answer:
->>>HEADER<- opcode: QUERY, status: NOERROR, id: 53242
Flags: qr rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL: 1

OPT PSEUDOSECTION:
DNS: version: 0, flags:; udp: 1232
QUESTION SECTION:
dell.com.                IN      NS

ANSWER SECTION:
dell.com.                600     IN      NS      ns1.us.dell.com.
dell.com.                600     IN      NS      ns3.us.dell.com.
dell.com.                600     IN      NS      ns4.us.dell.com.
dell.com.                600     IN      NS      ns5.us.dell.com.
dell.com.                600     IN      NS      ns6.us.dell.com.
dell.com.                600     IN      NS      ns2.us.dell.com.

Query time: 163 msec
SERVER: 1.1.1.1#53(1.1.1.1)
When: sab apr 30 17:28:08 CEST 2022
MSG SIZE rcvd: 148
```

I execute a single query of type `ns` to obtain the domain names of the authoritative Name Servers of the [Dell](#) (USA) Company. There are **six** different name servers associated with them, which belong to the same domain: `us.dell.com`. I think that the name server called `<ns1.us.dell.com>` (`143.166.82.251`) is the primary one, because of its name.

In order to get these IP addresses I executed another query with the `dig` command and with the `-f` option.

`dig -f names.txt`

```
davide@davide-hp:~$ dig -f names.txt +short
143.166.224.11
143.166.224.3
143.166.83.13
143.166.82.252
143.166.82.251
143.166.224.235
```

`whois dell.com`

```
davide@davide-hp:~$ whois dell.com
Domain Name: DELL.COM
Registry Domain ID: 1978972_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.safenames.net
Registrar URL: http://www.safenames.net
Updated Date: 2010-04-16T21:36:51Z
Creation Date: 1988-11-22T05:00:00Z
Registry Expiry Date: 2024-11-21T05:00:00Z
Registrar: SafeNames Ltd.
Registrar IANA ID: 447
Registrar Abuse Contact Email: abuse@safenames.net
Registrar Abuse Contact Phone: +44.1908200022
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.US.DELL.COM
Name Server: NS2.US.DELL.COM
Name Server: NS3.US.DELL.COM
Name Server: NS4.US.DELL.COM
Name Server: NS5.US.DELL.COM
Name Server: NS6.US.DELL.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-04-30T15:33:56Z <<<
```

*nslookup -type=soa dell.com*

```
davide@davide-hp:~$ nslookup -type=soa dell.com
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
dell.com
    origin = ns1.us.dell.com
    mail addr = hostmaster.dell.com
    serial = 629820137
    refresh = 900
    retry = 120
    expire = 604800
    minimum = 600

Authoritative answers can be found from:
```

The domain was registered by <SafeNames Ltd> on 22-11-1988 and will expire on 21-11-2024. Notice how the result of the *whois* command shows six name servers associated with the domain. The output of this command also supports the hypothesis that the primary name server is: <ns1.us.dell.com> (143.166.82.251). Using the *nslookup* command confirms the hypothesis that the primary name server is: <ns1.us.dell.com>.

## Question 5

*dig @143.166.82.251 samsung.com -t NS*

*dig @143.166.82.251 unipv.it -t NS*

```
davide@davide-hp:~$ dig @143.166.82.251 samsung.com -t NS
;<<<>> DiG 9.16.1-Ubuntu <<<>> @143.166.82.251 samsung.com -t NS
(1 server found)
;; global options: +cmd
;; Got answer:
-->HEADER<<- opcode: QUERY, status: REFUSED, id: 26088
; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 9ba3ae07011e71f7f84ef75b626d58b944f4077ee421e346 (good)
;; QUESTION SECTION:
;samsung.com.                IN      NS

;; Query time: 200 msec
;; SERVER: 143.166.82.251#53(143.166.82.251)
;; WHEN: sab apr 30 17:41:45 CEST 2022
;; MSG SIZE rcvd: 68
```

```
davide@davide-hp:~$ dig @143.166.82.251 unipv.it -t NS
;<<<>> DiG 9.16.1-Ubuntu <<<>> @143.166.82.251 unipv.it -t NS
(1 server found)
;; global options: +cmd
;; Got answer:
-->HEADER<<- opcode: QUERY, status: REFUSED, id: 11669
; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL:
; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: ba92c2b613aa8523e4a17676626d58fb8116d650de3b1d28 (good)
;; QUESTION SECTION:
unipv.it.                    IN      NS

;; Query time: 239 msec
;; SERVER: 143.166.82.251#53(143.166.82.251)
;; WHEN: sab apr 30 17:42:51 CEST 2022
;; MSG SIZE rcvd: 65
```

Using the IP address of the primary name server of the American company [Dell](#), both queries were rejected. Clearly this name server does not know and cannot resolve the given hostnames. In fact, querying this server with hostnames that are part of the domain, you can get an answer. Furthermore this name server is not a public name server, so it is legitimate that it does not make recursion queries to other name servers if requested from outside its domain. It is also not certain that this name server has enabled recursive queries.

## Performance/auditing experiments:

### Question 1

```
dnsping -s 8.8.8.8 -c 20 -t NS web.unipv.it
dnsping -s 8.8.8.8 -c 20 -t MX web.unipv.it
dnsping -s 8.8.8.8 -c 20 -t AAAA web.unipv.it
dnsping -s 8.8.8.8 -c 20 web.unipv.it
```

```
(kali@kali)-[~]
$ dnsping -s 8.8.8.8 -c 20 -t NS web.unipv.it

dnsping DNS: 8.8.8.8:53, hostname: web.unipv.it, proto: UDP, rdatatype: NS, flags: RD
88 bytes from 8.8.8.8: seq=1 time=260.968 ms
88 bytes from 8.8.8.8: seq=2 time=52.093 ms
88 bytes from 8.8.8.8: seq=3 time=76.397 ms
88 bytes from 8.8.8.8: seq=4 time=37.628 ms
88 bytes from 8.8.8.8: seq=5 time=38.614 ms
88 bytes from 8.8.8.8: seq=6 time=87.519 ms
88 bytes from 8.8.8.8: seq=7 time=61.310 ms
88 bytes from 8.8.8.8: seq=8 time=60.170 ms
88 bytes from 8.8.8.8: seq=9 time=109.214 ms
88 bytes from 8.8.8.8: seq=10 time=43.170 ms
88 bytes from 8.8.8.8: seq=11 time=100.429 ms
88 bytes from 8.8.8.8: seq=12 time=40.539 ms
88 bytes from 8.8.8.8: seq=13 time=106.573 ms
88 bytes from 8.8.8.8: seq=14 time=97.900 ms
88 bytes from 8.8.8.8: seq=15 time=45.901 ms
88 bytes from 8.8.8.8: seq=16 time=58.008 ms
88 bytes from 8.8.8.8: seq=17 time=61.741 ms
88 bytes from 8.8.8.8: seq=18 time=34.720 ms
88 bytes from 8.8.8.8: seq=19 time=33.905 ms
88 bytes from 8.8.8.8: seq=20 time=47.602 ms

--- 8.8.8.8 dnsping statistics ---
20 requests transmitted, 20 responses received, 0% lost
min=33.905 ms, avg=72.720 ms, max=260.968 ms, stddev=50.889 ms
```

The performance of the Google public name server is analyzed. The test was done by requesting 20 queries of type: NS / MX / AAAA / A, requested for the *unipv.it* domain. The results obtained are consistent with expectations. That is, in general, the RTT is higher when using a public name server than using the default one (assigned by the router). On the other

```
(kali@kali)-[~]
$ dnsping -s 8.8.8.8 -c 20 -t MX web.unipv.it

dnsping DNS: 8.8.8.8:53, hostname: web.unipv.it, proto: UDP, rdatatype: MX, flags: RD
88 bytes from 8.8.8.8: seq=1 time=71.627 ms
88 bytes from 8.8.8.8: seq=2 time=68.900 ms
88 bytes from 8.8.8.8: seq=3 time=180.531 ms
88 bytes from 8.8.8.8: seq=4 time=98.958 ms
88 bytes from 8.8.8.8: seq=5 time=43.905 ms
88 bytes from 8.8.8.8: seq=6 time=96.113 ms
88 bytes from 8.8.8.8: seq=7 time=62.570 ms
88 bytes from 8.8.8.8: seq=8 time=34.241 ms
88 bytes from 8.8.8.8: seq=9 time=36.103 ms
88 bytes from 8.8.8.8: seq=10 time=259.068 ms
88 bytes from 8.8.8.8: seq=11 time=44.839 ms
88 bytes from 8.8.8.8: seq=12 time=41.587 ms
88 bytes from 8.8.8.8: seq=13 time=77.897 ms
88 bytes from 8.8.8.8: seq=14 time=36.357 ms
88 bytes from 8.8.8.8: seq=15 time=36.716 ms
88 bytes from 8.8.8.8: seq=16 time=40.728 ms
88 bytes from 8.8.8.8: seq=17 time=35.882 ms
88 bytes from 8.8.8.8: seq=18 time=61.905 ms
88 bytes from 8.8.8.8: seq=19 time=32.951 ms
88 bytes from 8.8.8.8: seq=20 time=30.005 ms

--- 8.8.8.8 dnsping statistics ---
20 requests transmitted, 20 responses received, 0% lost
min=30.005 ms, avg=69.544 ms, max=259.068 ms, stddev=56.870 ms
```



hand, the high standard error value obtained was less expected. There are RTT values around 30ms but also values that touch 300ms.

```
(kali㉿kali)-[~]
$ dnsping -s 8.8.8.8 -c 20 -t AAAA web.unipv.it
dnsping DNS: 8.8.8.8:53, hostname: web.unipv.it, proto: UDP, rdatatype: AAAA, flags: RD
88 bytes from 8.8.8.8: seq=1    time=44.709 ms
88 bytes from 8.8.8.8: seq=2    time=59.880 ms
88 bytes from 8.8.8.8: seq=3    time=39.068 ms
88 bytes from 8.8.8.8: seq=4    time=35.699 ms
88 bytes from 8.8.8.8: seq=5    time=38.337 ms
88 bytes from 8.8.8.8: seq=6    time=59.174 ms
88 bytes from 8.8.8.8: seq=7    time=56.820 ms
88 bytes from 8.8.8.8: seq=8    time=130.194 ms
88 bytes from 8.8.8.8: seq=9    time=39.596 ms
88 bytes from 8.8.8.8: seq=10   time=106.441 ms
88 bytes from 8.8.8.8: seq=11   time=35.736 ms
88 bytes from 8.8.8.8: seq=12   time=30.004 ms
88 bytes from 8.8.8.8: seq=13   time=54.974 ms
88 bytes from 8.8.8.8: seq=14   time=43.486 ms
88 bytes from 8.8.8.8: seq=15   time=40.955 ms
88 bytes from 8.8.8.8: seq=16   time=30.954 ms
88 bytes from 8.8.8.8: seq=17   time=42.070 ms
88 bytes from 8.8.8.8: seq=18   time=108.630 ms
88 bytes from 8.8.8.8: seq=19   time=46.479 ms
88 bytes from 8.8.8.8: seq=20   time=28.378 ms

--- 8.8.8.8 dnsping statistics ---
20 requests transmitted, 20 responses received, 0% lost
min=28.378 ms, avg=53.579 ms, max=130.194 ms, stddev=28.359 ms
```

```
(kali㉿kali)-[~]
$ dnsping -s 8.8.8.8 -c 20 web.unipv.it
dnsping DNS: 8.8.8.8:53, hostname: web.unipv.it, proto: UDP, rdatatype: A, flags: RD
57 bytes from 8.8.8.8: seq=1    time=53.257 ms
57 bytes from 8.8.8.8: seq=2    time=35.287 ms
57 bytes from 8.8.8.8: seq=3    time=34.154 ms
57 bytes from 8.8.8.8: seq=4    time=36.882 ms
57 bytes from 8.8.8.8: seq=5    time=38.851 ms
57 bytes from 8.8.8.8: seq=6    time=80.256 ms
57 bytes from 8.8.8.8: seq=7    time=60.045 ms
57 bytes from 8.8.8.8: seq=8    time=34.366 ms
57 bytes from 8.8.8.8: seq=9    time=26.901 ms
57 bytes from 8.8.8.8: seq=10   time=296.235 ms
57 bytes from 8.8.8.8: seq=11   time=34.971 ms
57 bytes from 8.8.8.8: seq=12   time=33.513 ms
57 bytes from 8.8.8.8: seq=13   time=33.207 ms
57 bytes from 8.8.8.8: seq=14   time=34.363 ms
57 bytes from 8.8.8.8: seq=15   time=30.973 ms
57 bytes from 8.8.8.8: seq=16   time=38.910 ms
57 bytes from 8.8.8.8: seq=17   time=32.718 ms
57 bytes from 8.8.8.8: seq=18   time=91.684 ms
57 bytes from 8.8.8.8: seq=19   time=28.738 ms
57 bytes from 8.8.8.8: seq=20   time=31.056 ms

--- 8.8.8.8 dnsping statistics ---
20 requests transmitted, 20 responses received, 0% lost
min=26.901 ms, avg=54.318 ms, max=296.235 ms, stddev=59.464 ms
```

It is possible to see that the response time changes by varying the type of query. In general, type A queries (in this case smaller size) take less time. All the other three types tested have very similar times.

Finally it must be said that the results obtained were taken in a single moment, therefore their validity is limited. The analysis should be repeated several times to collect data closer to reality.

## Question 2

```
dnseval -f list-NS -t NS -c 20 berkeley.edu
dnseval -f list-NS -t MX -c 20 berkeley.edu
dnseval -f list-NS -t A -c 20 berkeley.edu
```

The public name servers that I have chosen to test for this part are the following, note that the geographical location is also shown, useful for considerations:

|                |           |
|----------------|-----------|
| 139.134.2.190  | Australia |
| 8.8.8.8        | USA       |
| 64.6.64.6      | USA       |
| 62.149.128.2   | Italy     |
| 200.221.11.101 | Brazil    |
| 82.103.129.72  | Denmark   |

For each name server 50 queries were made, of type A / MX / NS. The hostnames used are the following:

- web.unipv.it
- australia.gov.au
- fbi.gov
- verizion.com
- berkeley.edu

```
(kali@kali)-[~]
$ dnseval -f list-NS -t A -c 50 web.unipv.it
```

| server         | avg(ms) | min(ms) | max(ms) | stddev(ms) | lost(%) | ttl | flags                | response |
|----------------|---------|---------|---------|------------|---------|-----|----------------------|----------|
| 139.134.2.190  | 351.433 | 320.234 | 980.675 | 92.084     | %0      | 283 | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 43.744  | 25.964  | 82.025  | 10.509     | %0      | 215 | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 60.542  | 46.290  | 156.426 | 23.257     | %0      | 297 | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 50.720  | 37.128  | 81.172  | 7.757      | %0      | 297 | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 265.851 | 238.248 | 523.538 | 53.170     | %0      | 288 | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 80.144  | 64.013  | 138.715 | 19.143     | %4      | 298 | QR -- -- RD RA -- -- | NOERROR  |

```
(kali@kali)-[~]
$ dnseval -f list-NS -t MX -c 50 web.unipv.it
```

| server         | avg(ms) | min(ms) | max(ms) | stddev(ms) | lost(%) | ttl | flags                | response |
|----------------|---------|---------|---------|------------|---------|-----|----------------------|----------|
| 139.134.2.190  | 340.975 | 319.217 | 776.955 | 63.351     | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 41.475  | 26.503  | 83.560  | 16.104     | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 55.979  | 47.276  | 104.691 | 11.753     | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 48.818  | 36.179  | 74.393  | 7.580      | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 260.720 | 236.250 | 488.346 | 46.561     | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 80.090  | 65.580  | 178.483 | 25.262     | %4      | N/A | QR -- -- RD RA -- -- | NOERROR  |

```
(kali@kali)-[~]
$ dnseval -f list-NS -t NS -c 50 web.unipv.it
```

| server         | avg(ms) | min(ms) | max(ms)  | stddev(ms) | lost(%) | ttl | flags                | response |
|----------------|---------|---------|----------|------------|---------|-----|----------------------|----------|
| 139.134.2.190  | 352.343 | 320.147 | 1151.736 | 115.657    | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 33.132  | 26.123  | 52.916   | 6.739      | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 62.573  | 48.002  | 102.244  | 13.858     | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 68.476  | 42.894  | 96.840   | 6.172      | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 261.646 | 237.926 | 487.588  | 47.068     | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 77.645  | 64.718  | 125.200  | 14.703     | %4      | N/A | QR -- -- RD RA -- -- | NOERROR  |



```
(kali@kali)-[~]
$ dnseval -f list-NS -t A -c 50 australia.gov.au
```

| server         | avg(ms) | min(ms) | max(ms) | stddev(ms) | lost(%) | ttl  | flags                | response |
|----------------|---------|---------|---------|------------|---------|------|----------------------|----------|
| 139.134.2.190  | 337.268 | 321.707 | 432.806 | 17.523     | %0      | 3583 | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 55.019  | 26.850  | 264.366 | 34.752     | %0      | 3598 | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 83.629  | 46.669  | 883.306 | 122.698    | %0      | 3597 | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 50.477  | 35.523  | 100.734 | 11.494     | %0      | 3597 | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 263.424 | 241.763 | 455.845 | 39.966     | %0      | 3587 | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 86.279  | 63.704  | 255.181 | 40.967     | %4      | 3598 | QR -- -- RD RA -- -- | NOERROR  |

```
(kali@kali)-[~]
$ dnseval -f list-NS -t MX -c 50 australia.gov.au
```

| server         | avg(ms) | min(ms) | max(ms) | stddev(ms) | lost(%) | ttl | flags                | response |
|----------------|---------|---------|---------|------------|---------|-----|----------------------|----------|
| 139.134.2.190  | 335.895 | 322.281 | 457.078 | 18.391     | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 39.191  | 27.047  | 96.121  | 17.107     | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 59.917  | 46.876  | 121.888 | 15.727     | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 50.212  | 39.258  | 86.043  | 9.057      | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 262.575 | 237.056 | 384.329 | 25.270     | %0      | N/A | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 75.694  | 62.940  | 117.577 | 12.007     | %4      | N/A | QR -- -- RD RA -- -- | NOERROR  |

```
(kali@kali)-[~]
$ dnseval -f list-NS -t NS -c 50 australia.gov.au
```

| server         | avg(ms) | min(ms) | max(ms) | stddev(ms) | lost(%) | ttl    | flags                | response |
|----------------|---------|---------|---------|------------|---------|--------|----------------------|----------|
| 139.134.2.190  | 342.082 | 322.152 | 474.109 | 24.608     | %0      | 383    | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 43.323  | 25.634  | 251.538 | 38.765     | %0      | 21598  | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 64.219  | 48.578  | 120.578 | 15.689     | %0      | 43197  | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 50.779  | 37.000  | 100.428 | 9.484      | %0      | 86397  | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 260.006 | 240.718 | 383.699 | 25.714     | %0      | 172787 | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 76.083  | 62.476  | 118.820 | 11.855     | %4      | 172799 | QR -- -- RD RA -- -- | NOERROR  |

```
(kali@kali)-[~]
$ dnseval -f list-NS -t A -c 50 verizon.com
```

| server         | avg(ms) | min(ms) | max(ms) | stddev(ms) | lost(%) | ttl | flags                | response |
|----------------|---------|---------|---------|------------|---------|-----|----------------------|----------|
| 139.134.2.190  | 341.315 | 323.724 | 376.713 | 15.113     | %0      | 584 | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 34.649  | 26.479  | 56.069  | 7.771      | %0      | 599 | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 63.127  | 47.939  | 111.278 | 12.558     | %0      | 596 | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 49.751  | 36.722  | 71.012  | 7.692      | %0      | 28  | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 265.615 | 237.345 | 505.879 | 41.733     | %0      | 392 | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 77.044  | 62.333  | 99.916  | 10.200     | %4      | 599 | QR -- -- RD RA -- -- | NOERROR  |

```
(kali@kali)-[~]
$ dnseval -f list-NS -t MX -c 50 verizon.com
```

| server         | avg(ms) | min(ms) | max(ms) | stddev(ms) | lost(%) | ttl | flags                | response |
|----------------|---------|---------|---------|------------|---------|-----|----------------------|----------|
| 139.134.2.190  | 336.752 | 321.575 | 364.995 | 7.045      | %0      | 583 | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 35.242  | 26.433  | 52.073  | 8.215      | %0      | 598 | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 56.134  | 47.083  | 75.776  | 6.936      | %0      | 597 | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 48.124  | 35.717  | 69.232  | 7.141      | %0      | 598 | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 263.750 | 239.816 | 367.576 | 25.364     | %0      | 586 | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 75.738  | 63.094  | 99.627  | 9.658      | %4      | 599 | QR -- -- RD RA -- -- | NOERROR  |

```
(kali@kali)-[~]
$ dnseval -f list-NS -t NS -c 50 verizon.com
```

| server         | avg(ms) | min(ms) | max(ms) | stddev(ms) | lost(%) | ttl  | flags                | response |
|----------------|---------|---------|---------|------------|---------|------|----------------------|----------|
| 139.134.2.190  | 333.806 | 322.217 | 404.946 | 12.977     | %0      | 3477 | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 37.881  | 27.269  | 54.840  | 7.809      | %0      | 3598 | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 58.405  | 47.422  | 76.099  | 7.231      | %0      | 3597 | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 49.266  | 36.825  | 75.099  | 6.628      | %0      | 27   | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 261.187 | 239.912 | 395.400 | 26.167     | %0      | 3588 | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 78.698  | 62.736  | 102.599 | 11.484     | %4      | 3598 | QR -- -- RD RA -- -- | NOERROR  |

```
(kali@kali)-[~]
$ dnseval -f list-NS -t A -c 50 fbi.gov
```

| server         | avg(ms) | min(ms) | max(ms) | stddev(ms) | lost(%) | ttl | flags                | response |
|----------------|---------|---------|---------|------------|---------|-----|----------------------|----------|
| 139.134.2.190  | 341.843 | 322.144 | 453.433 | 19.758     | %0      | 103 | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 36.708  | 26.300  | 100.999 | 14.166     | %0      | 118 | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 61.643  | 47.939  | 135.366 | 19.081     | %0      | 117 | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 50.339  | 37.427  | 88.788  | 8.501      | %0      | 117 | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 266.316 | 237.988 | 578.547 | 61.102     | %0      | 108 | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 83.932  | 62.511  | 289.117 | 49.165     | %4      | 298 | QR -- -- RD RA -- -- | NOERROR  |

```
(kali@kali)-[~]
$ dnseval -f list-NS -t MX -c 50 fbi.gov
```

| server         | avg(ms) | min(ms) | max(ms) | stddev(ms) | lost(%) | ttl | flags                | response |
|----------------|---------|---------|---------|------------|---------|-----|----------------------|----------|
| 139.134.2.190  | 351.317 | 320.628 | 463.002 | 25.923     | %0      | 103 | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 37.455  | 26.285  | 112.407 | 16.124     | %0      | 118 | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 59.165  | 47.410  | 115.770 | 14.611     | %0      | 117 | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 51.687  | 36.216  | 95.287  | 12.259     | %0      | 117 | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 262.047 | 238.140 | 392.278 | 27.725     | %0      | 108 | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 77.620  | 65.013  | 106.063 | 9.947      | %4      | 298 | QR -- -- RD RA -- -- | NOERROR  |

```
(kali@kali)-[~]
$ dnseval -f list-NS -t NS -c 50 fbi.gov
```

| server         | avg(ms) | min(ms) | max(ms) | stddev(ms) | lost(%) | ttl | flags                | response |
|----------------|---------|---------|---------|------------|---------|-----|----------------------|----------|
| 139.134.2.190  | 349.118 | 321.899 | 467.521 | 24.852     | %0      | 583 | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 37.580  | 26.208  | 90.518  | 13.383     | %0      | 598 | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 62.997  | 47.579  | 94.493  | 10.468     | %0      | 597 | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 49.473  | 35.921  | 75.332  | 7.165      | %0      | 598 | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 261.617 | 237.910 | 386.371 | 25.788     | %0      | 588 | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 77.796  | 62.433  | 112.103 | 14.052     | %4      | 598 | QR -- -- RD RA -- -- | NOERROR  |

```
(kali@kali)-[~]
$ dnseval -f list-NS -t A -c 50 berkeley.edu
```

| server         | avg(ms) | min(ms) | max(ms) | stddev(ms) | lost(%) | ttl | flags                | response |
|----------------|---------|---------|---------|------------|---------|-----|----------------------|----------|
| 139.134.2.190  | 341.917 | 320.577 | 531.408 | 31.473     | %0      | 283 | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 53.854  | 26.931  | 210.883 | 55.019     | %0      | 297 | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 170.412 | 56.613  | 226.749 | 79.987     | %14     | 300 | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 55.127  | 36.870  | 219.798 | 35.041     | %0      | 297 | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 264.086 | 243.127 | 472.822 | 40.475     | %0      | 287 | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 81.738  | 64.098  | 246.089 | 39.251     | %4      | 298 | QR -- -- RD RA -- -- | NOERROR  |

```
(kali@kali)-[~]
$ dnseval -f list-NS -t MX -c 50 berkeley.edu
```

| server         | avg(ms) | min(ms) | max(ms) | stddev(ms) | lost(%) | ttl | flags                | response |
|----------------|---------|---------|---------|------------|---------|-----|----------------------|----------|
| 139.134.2.190  | 340.099 | 320.144 | 521.034 | 28.701     | %0      | 255 | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 50.577  | 25.681  | 225.595 | 52.782     | %0      | 269 | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 72.448  | 47.431  | 233.063 | 44.951     | %0      | 267 | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 54.267  | 37.106  | 225.481 | 35.112     | %0      | 268 | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 269.396 | 239.262 | 534.875 | 54.773     | %0      | 259 | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 86.138  | 66.975  | 250.121 | 39.299     | %4      | 298 | QR -- -- RD RA -- -- | NOERROR  |

```
(kali@kali)-[~]
$ dnseval -f list-NS -t NS -c 50 berkeley.edu
```

| server         | avg(ms) | min(ms) | max(ms) | stddev(ms) | lost(%) | ttl   | flags                | response |
|----------------|---------|---------|---------|------------|---------|-------|----------------------|----------|
| 139.134.2.190  | 334.899 | 320.741 | 353.020 | 6.839      | %0      | 9298  | QR -- -- RD RA -- -- | NOERROR  |
| 8.8.8.8        | 50.562  | 26.498  | 210.708 | 51.678     | %0      | 10798 | QR -- -- RD RA -- -- | NOERROR  |
| 64.6.64.6      | 57.410  | 46.990  | 85.677  | 7.301      | %0      | 8935  | QR -- -- RD RA -- -- | NOERROR  |
| 62.149.128.2   | 48.539  | 37.362  | 60.955  | 5.627      | %0      | 9300  | QR -- -- RD RA -- -- | NOERROR  |
| 200.221.11.101 | 255.562 | 245.607 | 272.766 | 6.038      | %0      | 9288  | QR -- -- RD RA -- -- | NOERROR  |
| 82.103.129.72  | 80.869  | 63.424  | 244.517 | 38.902     | %4      | 10799 | QR -- -- RD RA -- -- | NOERROR  |

What the data shows is that the times obtained vary greatly depending on the name server used, as might be expected. It is clear that performance is greatly influenced by the geographic location of the name server, in fact for the same query a name server in Australia takes up to six times the time of a name server in Italy. With the same name server, I expected a big time difference based on the type of query requested. In reality the results obtained go against this expectation, there are small variations in times.

### Question 3

The public name servers that I have chosen to test for this part are the following, note that the geographical location is also shown, useful for considerations:

|                |           |
|----------------|-----------|
| 139.134.2.190  | Australia |
| 8.8.8.8        | USA       |
| 64.6.64.6      | USA       |
| 200.221.11.101 | Brazil    |
| 82.103.129.72  | Denmark   |

```
sudo dnstraceroute -x -a -s 139.134.2.190 unipv.it
```

The results thus obtained are consistent with those expected. There are some things in common with all name servers used, for example in hops 5/6/7 routers obscure responses to this type of traffic. This being a common behavior with every query run, I can imagine that it is related to my ISP. The same consideration can be made for all 10 first hops, they are all in common. Regardless of the name server used. In particular, all the queries are in my ISP's network at least up to hop 11, some of these even up to hop 13. Hop number 11 varies each time, but is always within the ISP's network.

```
(kali@kali)~$ sudo dnstraceroute -x -a -s 139.134.2.190 unipv.it
dnstraceroute DNS: 139.134.2.190:53, hostname: unipv.it, rdatatype: A
1 10.0.2.2 (10.0.2.2) 1.026 ms
2 _gateway (192.168.75.166) 8.501 ms
3 192.168.60.82 (192.168.60.82) 40.402 ms
4 192.168.60.82 (192.168.60.82) 31.579 ms
5 *
6 *
7 *
8 10.178.86.49 (10.178.86.49) 81.799 ms
9 83.224.40.186 (83.224.40.186) 38.711 ms
10 83.224.40.185 (83.224.40.185) 56.547 ms
11 ae3-100-xcr1.mlb.cw.net (195.59.1.85) [AS1273 CW Vodafone Group PLC, EU] 34.511 ms
12 ae9-tcr1.pat.cw.net (195.2.9.89) [AS1273 CW Vodafone Group PLC, EU] 55.039 ms
13 ae.29-xcr1.hex.cw.net (195.2.9.94) [AS1273 CW Vodafone Group PLC, EU] 55.797 ms
14 ae9-xcr1.lnt.cw.net (195.2.24.161) [AS1273 CW Vodafone Group PLC, EU] 48.968 ms
15 195.66.224.177 (195.66.224.177) 57.191 ms
16 i-1001.ulhc-core02.telstraglobal.net (202.84.178.70) [AS4637 ASN-TELSTRA-GLOBAL Telstra Global, HK] 73.708 ms
17 202.84.249.82 (202.84.249.82) [AS4637 ASN-TELSTRA-GLOBAL Telstra Global, HK] 189.057 ms
18 202.84.249.81 (202.84.249.81) [AS4637 ASN-TELSTRA-GLOBAL Telstra Global, HK] 189.542 ms
19 202.84.249.81 (202.84.249.81) [AS4637 ASN-TELSTRA-GLOBAL Telstra Global, HK] 328.251 ms
20 i-37.sydo-core03.telstraglobal.net (202.84.247.46) [AS4637 ASN-TELSTRA-GLOBAL Telstra Global, HK] 330.275 ms
21 bundle-ether3.oxf-gw11.sydney.telstra.net (203.50.13.97) [AS1221 ASN-TELSTRA Telstra Corporation Ltd, AU] 331.119 ms
22 bundle-ether1.chw-core10.sydney.telstra.net (203.50.6.92) [AS1221 ASN-TELSTRA Telstra Corporation Ltd, AU] 330.707 ms
23 Bundle-Ether1.civ-core30.canberra.telstra.net (203.50.6.112) [AS1221 ASN-TELSTRA Telstra Corporation Ltd, AU] 328.426 ms
24 Bundle-Ether1.civ-dlr20.canberra.telstra.net (203.50.8.9) [AS1221 ASN-TELSTRA Telstra Corporation Ltd, AU] 339.105 ms
25 139.134.2.190 (139.134.2.190) [AS1221 ASN-TELSTRA Telstra Corporation Ltd, AU] 1275.103 ms
```

Starting with hop 12 the behavior changes significantly depending on the specified server. Sometimes this is an exchange point, while other times it's still a router within my ISP's network.

```
(kali㉿kali)-[~]
$ sudo dnstraceroute -x -a -s 8.8.8.8 unipv.it
dnstraceroute DNS: 8.8.8.8:53, hostname: unipv.it, rdatatype: A
1      10.0.2.2 (10.0.2.2) 1.330 ms
2      _gateway (192.168.75.166) 3.767 ms
3      192.168.60.82 (192.168.60.82) 243.534 ms
4      192.168.60.82 (192.168.60.82) 79.703 ms
5      *
6      192.168.0.69 (192.168.0.69) 30.718 ms
7      *
8      10.178.86.49 (10.178.86.49) 81.967 ms
9      83.224.40.186 (83.224.40.186) 40.947 ms
10     83.224.40.185 (83.224.40.185) 34.057 ms
11     83.224.46.233 (83.224.46.233) 33.164 ms
12     216.239.49.41 (216.239.49.41) [AS15169 GOOGLE, US] 42.086 ms
13     142.251.235.179 (142.251.235.179) [AS15169 GOOGLE, US] 31.324 ms
14     dns.google (8.8.8.8) [AS15169 GOOGLE, US] 44.644 ms
```

```
(kali㉿kali)-[~]
$ sudo dnstraceroute -x -a -s 64.6.64.6 unipv.it
dnstraceroute DNS: 64.6.64.6:53, hostname: unipv.it, rdatatype: A
1      10.0.2.2 (10.0.2.2) 1.066 ms
2      _gateway (192.168.75.166) 6.236 ms
3      192.168.60.82 (192.168.60.82) 253.313 ms
4      192.168.60.82 (192.168.60.82) 31.297 ms
5      *
6      192.168.0.69 (192.168.0.69) 43.074 ms
7      *
8      10.178.86.49 (10.178.86.49) 70.373 ms
9      83.224.40.186 (83.224.40.186) 43.933 ms
10     83.224.40.185 (83.224.40.185) 42.353 ms
11     185.210.48.137 (185.210.48.137) 62.430 ms
12     lag17.fr4.mrs1.llnw.net (87.248.216.248) [AS22822 LLNW, US] 47.501 ms
13     p1-4.fr3.mrs1.llnw.net (178.79.236.9) [AS22822 LLNW, US] 52.344 ms
14     lag19.fr3.toj1.llnw.net (87.248.220.11) [AS22822 LLNW, US] 52.951 ms
15     uldns.p1-8-10g.fr3.toj1.llnw.net (95.140.224.29) [AS22822 LLNW, US] 65.003 ms
16     rec1pubns1.ultradns.net (64.6.64.6) [AS397213 ULTRADNS, US] 111.655 ms
```

```
(kali㉿kali)-[~]
$ sudo dnstraceroute -x -a -s 200.221.11.101 unipv.it
dnstraceroute DNS: 200.221.11.101:53, hostname: unipv.it, rdatatype: A
1      10.0.2.2 (10.0.2.2) 1.321 ms
2      _gateway (192.168.75.166) 7.429 ms
3      192.168.60.82 (192.168.60.82) 306.411 ms
4      192.168.60.82 (192.168.60.82) 62.099 ms
5      *
6      *
7      *
8      10.178.86.49 (10.178.86.49) 34.584 ms
9      83.224.40.186 (83.224.40.186) 53.655 ms
10     83.224.40.185 (83.224.40.185) 70.188 ms
11     ae3-100-xcr1.mlb.cw.net (195.59.1.85) [AS1273 CW Vodafone Group PLC, EU] 62.389 ms
12     ae23-xcr1.mrx.cw.net (195.2.31.118) [AS1273 CW Vodafone Group PLC, EU] 38.171 ms
13     as6762-gw-xcr1.mrx.cw.net (195.2.29.182) [AS1273 CW Vodafone Group PLC, EU] 41.718 ms
14     *
15     tim-brasil.sanpaolo8.spa.seabone.net (195.22.219.33) [AS6762 SEABONE-NET TELECOM ITALIA SPARKLE S.p.A., IT] 289.857 ms
16     26.252.40.189.isp.timbrasil.com.br (189.40.252.26) [AS26615 TIM SA, BR] 250.672 ms
17     *
18     186.234.29.38 (186.234.29.38) [AS7162 Universo Online S.A., BR] 251.799 ms
19     200-147-26-38.static.uol.com.br (200.147.26.38) [AS7162 Universo Online S.A., BR] 425.232 ms
20     ravel.uol.com.br (200.221.11.101) [AS7162 Universo Online S.A., BR] 272.105 ms
```

```
=== Expert Hints ===
[*] No expert hint available for this trace
```