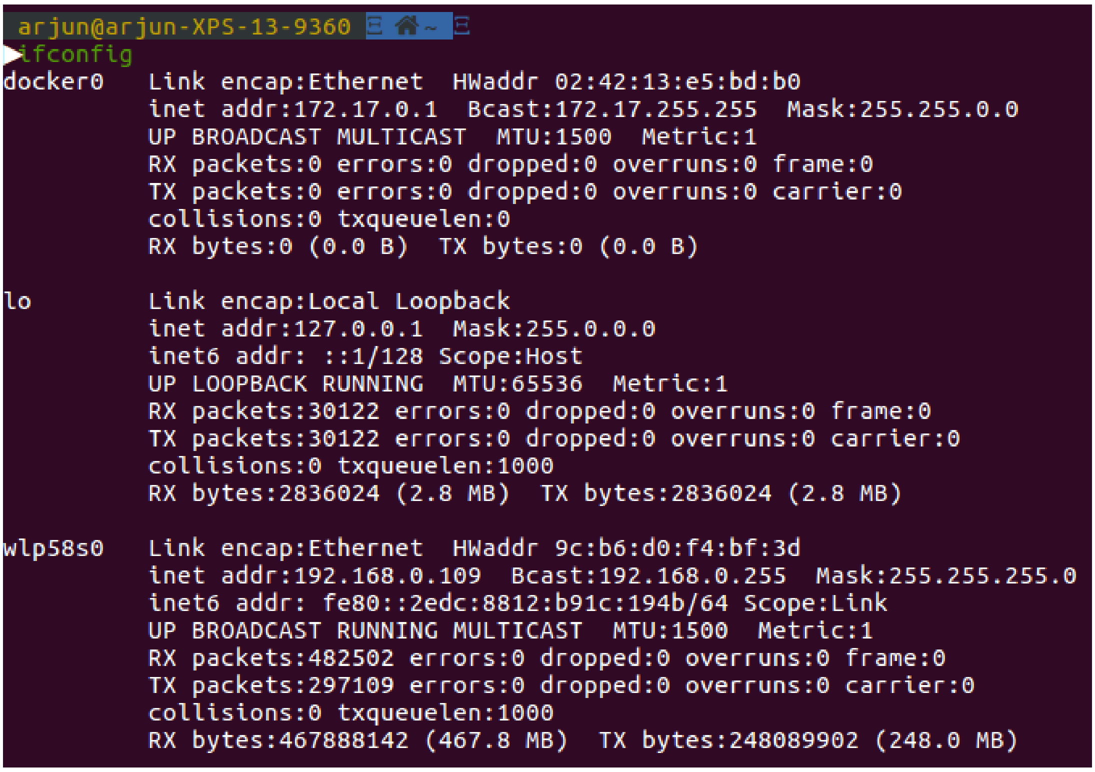
CS3205: INTRODUCTION TO COMPUTER NETWORKS
ASSIGNMENT 4

ARJUN BHARAT,CS17B006

INTRODUCTION

The aim of the assignment was to obtain the canonical names of websites by using nslookup. A study of mail servers associated with specific websites was also done.

1. IP AND MAC ADDRESS OF THE SYSTEM:



```
arjun@arjun-XPS-13-9360  ~
▶ifconfig
docker0   Link encap:Ethernet  HWaddr 02:42:13:e5:bd:b0
          inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:30122 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30122 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2836024 (2.8 MB)  TX bytes:2836024 (2.8 MB)

wlp58s0   Link encap:Ethernet  HWaddr 9c:b6:d0:f4:bf:3d
          inet addr:192.168.0.109  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::2edc:8812:b91c:194b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:482502 errors:0 dropped:0 overruns:0 frame:0
          TX packets:297109 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:467888142 (467.8 MB)  TX bytes:248089902 (248.0 MB)
```

A WiFi network was used, and hence the IP address is given by the **wlp58s0** filter.

2. DOMAINS USED FOR THIS ASSIGNMENT:

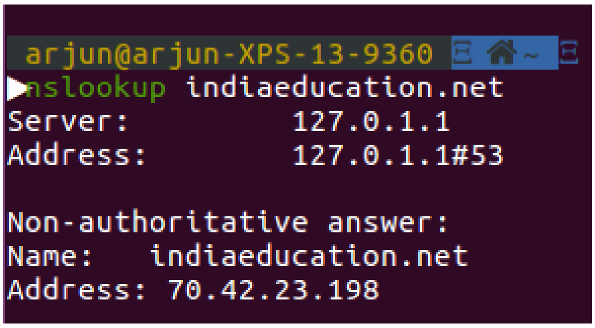
The following webistes were used for the assignment:

- www.indiaeducation.net
- www.tu-darmstadt.de
- www.umich.edu
- www.goidirectory.nic.in
- www.ifsr.in
- www.myntra.com
- www.inferno.fitness
- www.just.jobs
- www.nzherald.co.nz
- www.snet.lu

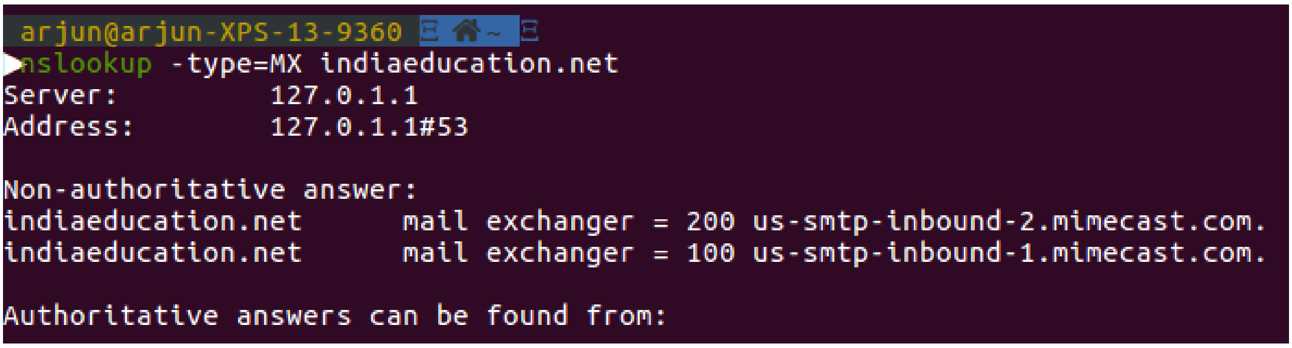
3. RESULTS OF THE TESTS PERFORMED

The results of the tests are summarised , website by website as follows:

a) For www.indiaeducation.net



```
arjun@arjun-XPS-13-9360  ~
▶nslookup indiaeducation.net
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   indiaeducation.net
Address: 70.42.23.198
```

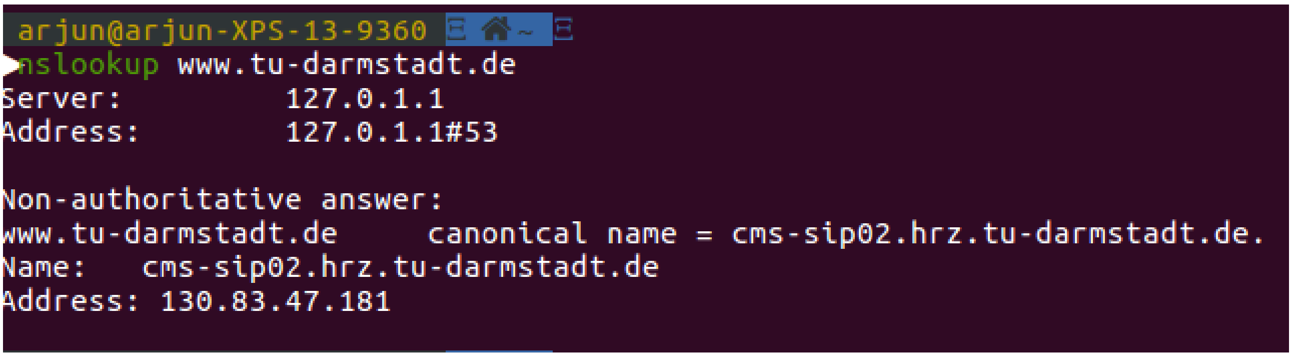


```
arjun@arjun-XPS-13-9360  ~
▶nslookup -type=MX indiaeducation.net
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
indiaeducation.net      mail exchanger = 200 us-smtp-inbound-2.mimecast.com.
indiaeducation.net      mail exchanger = 100 us-smtp-inbound-1.mimecast.com.

Authoritative answers can be found from:
```

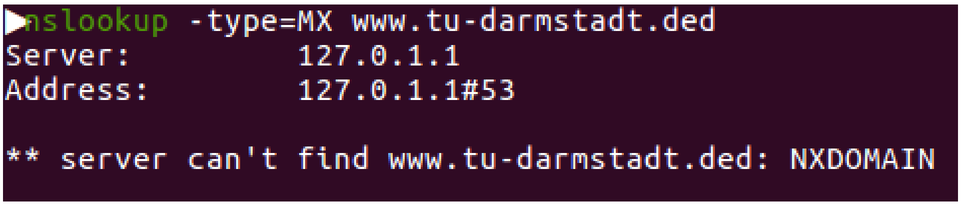
Observations:

There are 2 primary mail exchange servers used. Both are likely mirror webistes to reduce the load. This webiste has no canonical name.

b) For www.tu-darmstadt.de



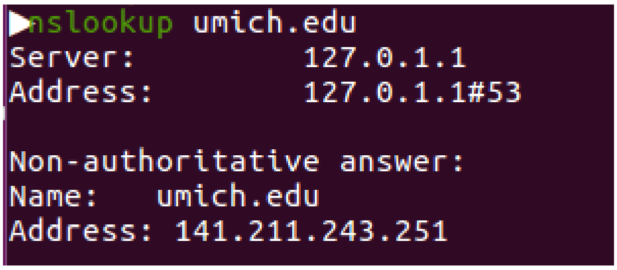
```
arjun@arjun-XPS-13-9360  ~
▶nslookup www.tu-darmstadt.de
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
www.tu-darmstadt.de     canonical name = cms-sip02.hrz.tu-darmstadt.de.
Name:   cms-sip02.hrz.tu-darmstadt.de
Address: 130.83.47.181
```



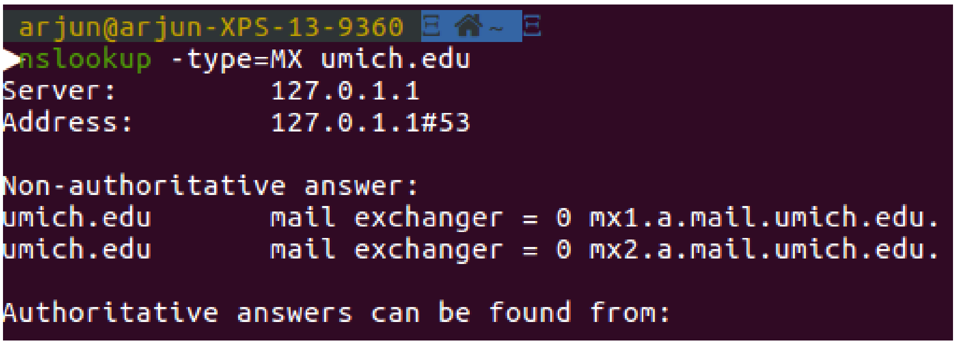
```
▶nslookup -type=MX www.tu-darmstadt.ded
Server:         127.0.1.1
Address:        127.0.1.1#53

** server can't find www.tu-darmstadt.ded: NXDOMAIN
```

Observation:
The website has a canonical name as depicted. However, no mail server exists for this educational website.

c) For www.umich.edu



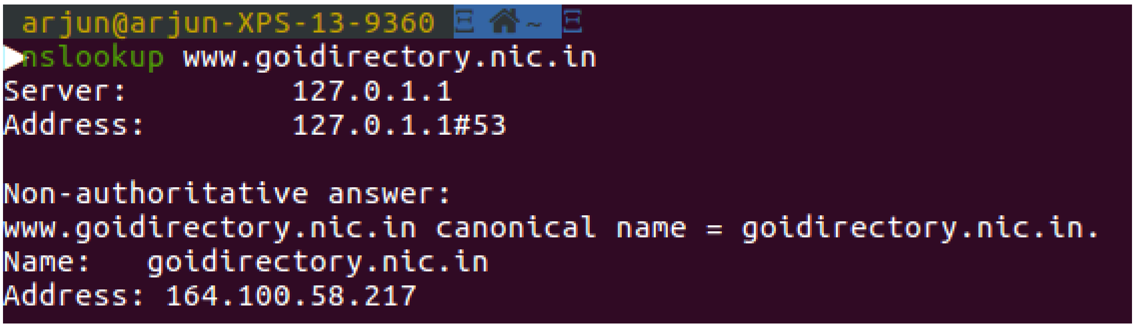
```
nslookup umich.edu
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   umich.edu
Address: 141.211.243.251
```



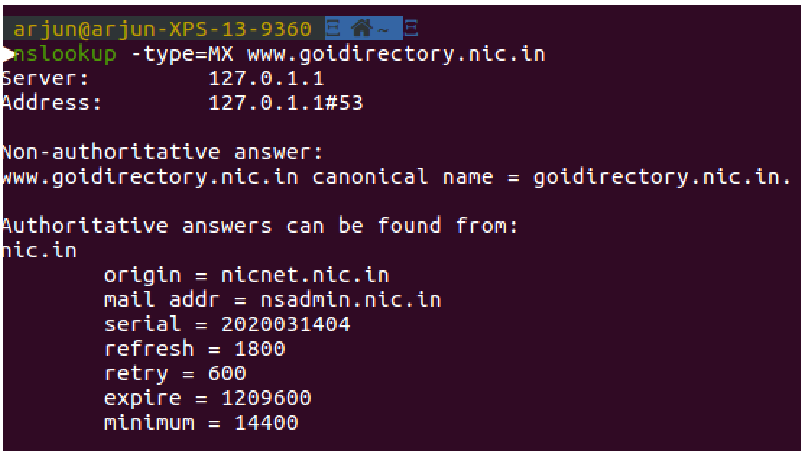
```
arjun@arjun-XPS-13-9360 ~
nslookup -type=MX umich.edu
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
umich.edu       mail exchanger = 0 mx1.a.mail.umich.edu.
umich.edu       mail exchanger = 0 mx2.a.mail.umich.edu.

Authoritative answers can be found from:
```

Observations:
There are 2 mail servers for this educational webiste in North America. However, no canonical aliases exist.

d) For www.goidirectory.nic.in



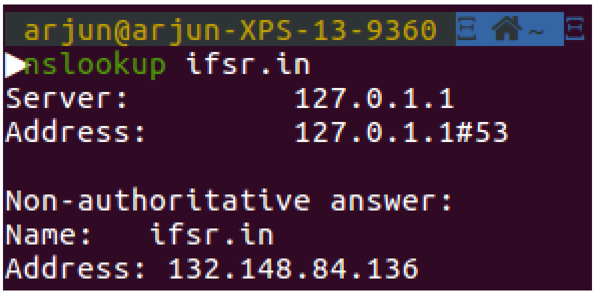
```
arjun@arjun-XPS-13-9360 ~
nslookup www.goidirectory.nic.in
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
www.goidirectory.nic.in canonical name = goidirectory.nic.in.
Name:   goidirectory.nic.in
Address: 164.100.58.217
```



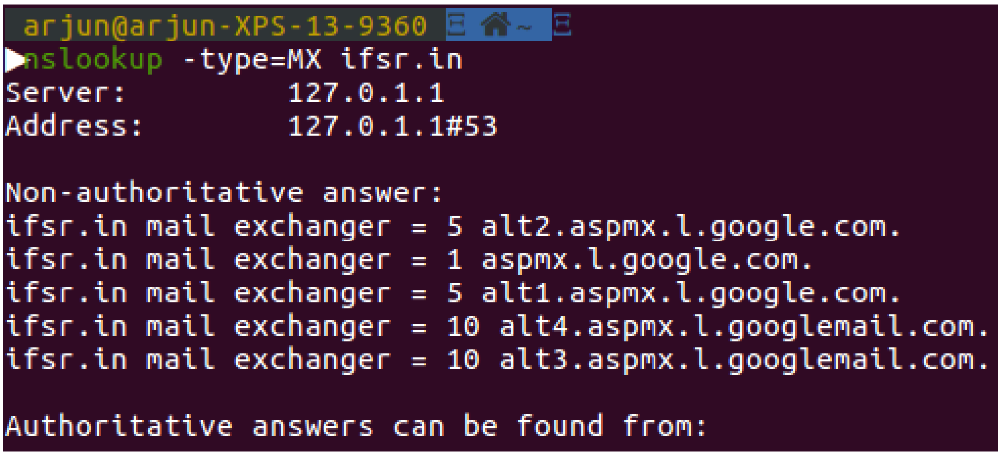
```
arjun@arjun-XPS-13-9360 ~
nslookup -type=MX www.goidirectory.nic.in
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
www.goidirectory.nic.in canonical name = goidirectory.nic.in.

Authoritative answers can be found from:
nic.in
        origin = nicnet.nic.in
        mail addr = nsadmin.nic.in
        serial = 2020031404
        refresh = 1800
        retry = 600
        expire = 1209600
        minimum = 14400
```

Observations:
The canonical name of the webiste is the same as its original name. An authorative answer was not obtained for this website.

e) For www.ifsr.in



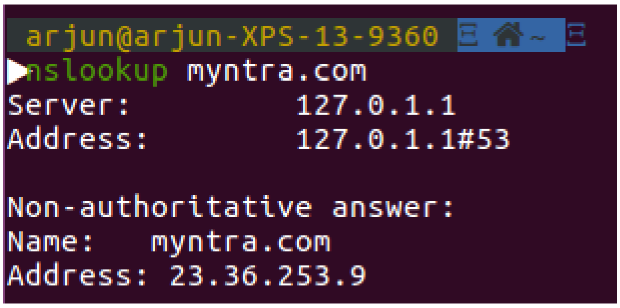
```
 arjun@arjun-XPS-13-9360  ~ 
▶nslookup ifsr.in
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   ifsr.in
Address: 132.148.84.136
```



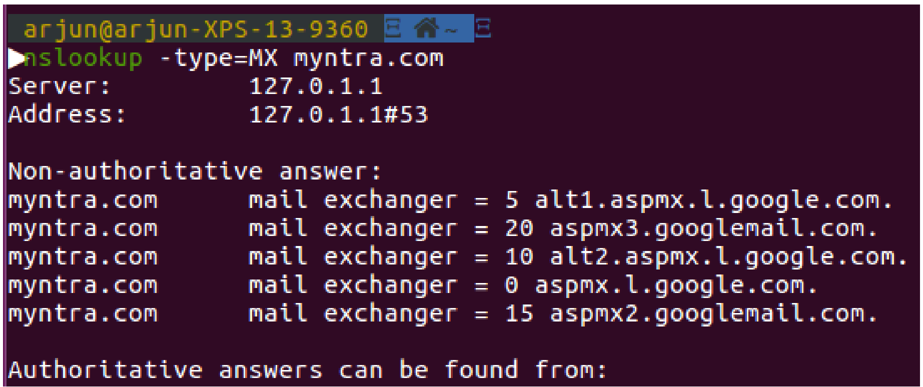
```
 arjun@arjun-XPS-13-9360  ~ 
▶nslookup -type=MX ifsr.in
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
ifsr.in mail exchanger = 5 alt2.aspmx.l.google.com.
ifsr.in mail exchanger = 1 aspmx.l.google.com.
ifsr.in mail exchanger = 5 alt1.aspmx.l.google.com.
ifsr.in mail exchanger = 10 alt4.aspmx.l.googlemail.com.
ifsr.in mail exchanger = 10 alt3.aspmx.l.googlemail.com.

Authoritative answers can be found from:
```

Observations:
There are no canonical names and 5 available mail servers.

f) For www.myntra.com



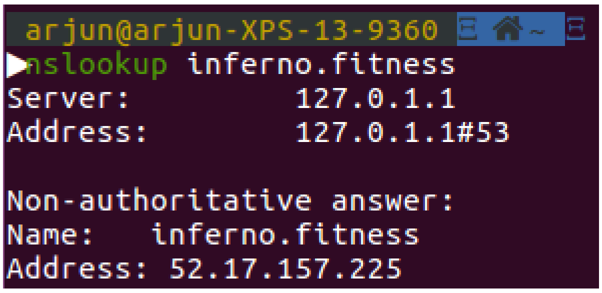
```
 arjun@arjun-XPS-13-9360  ~ 
▶nslookup myntra.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   myntra.com
Address: 23.36.253.9
```



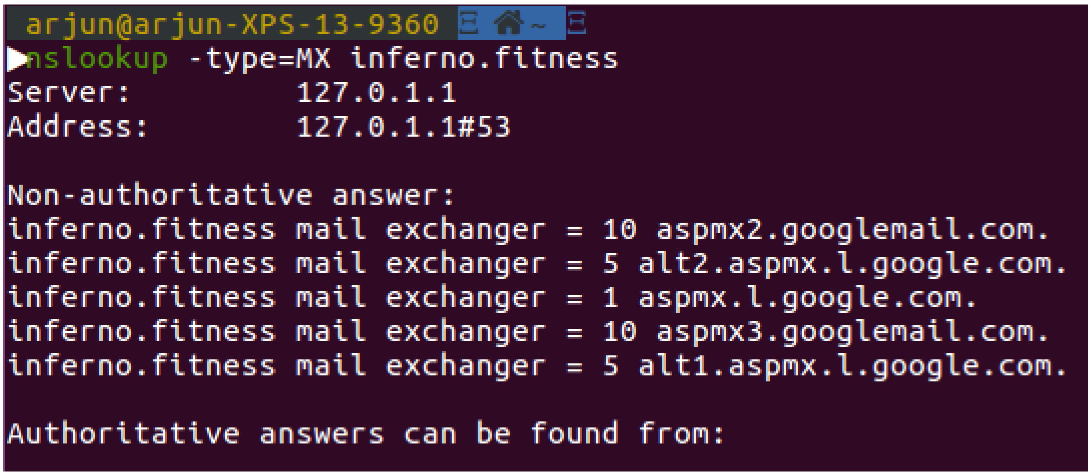
```
 arjun@arjun-XPS-13-9360  ~ 
▶nslookup -type=MX myntra.com
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
myntra.com      mail exchanger = 5 alt1.aspmx.l.google.com.
myntra.com      mail exchanger = 20 aspmx3.googlemail.com.
myntra.com      mail exchanger = 10 alt2.aspmx.l.google.com.
myntra.com      mail exchanger = 0 aspmx.l.google.com.
myntra.com      mail exchanger = 15 aspmx2.googlemail.com.

Authoritative answers can be found from:
```

Observations:
This shopping website has 5 mail servers possibly due to heavy concurrent load.

g) For www.inferno.fitness



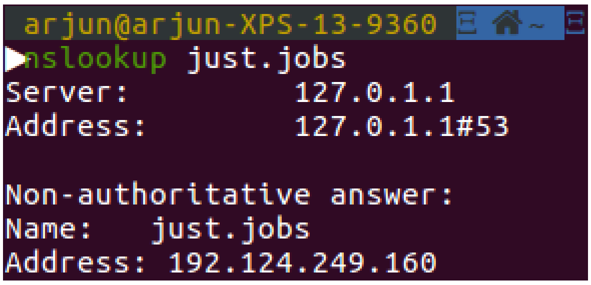
```
arjun@arjun-XPS-13-9360 ~
nslookup inferno.fitness
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   inferno.fitness
Address: 52.17.157.225
```



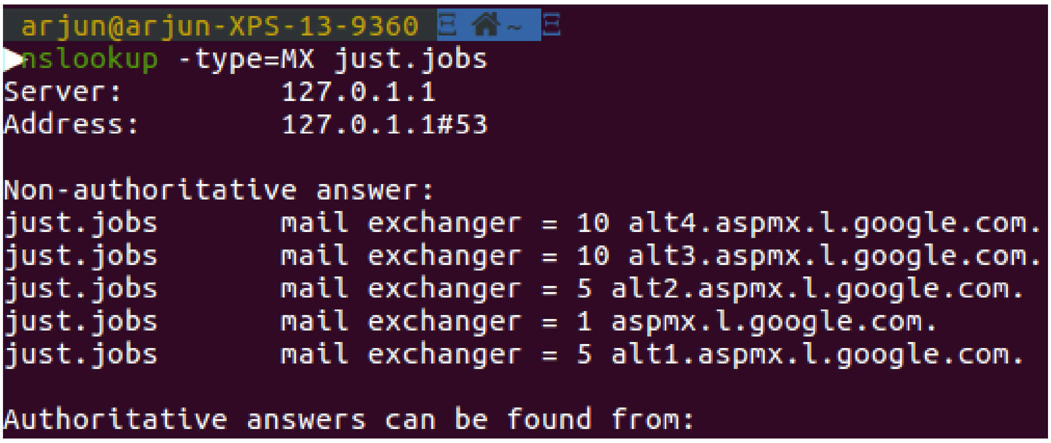
```
arjun@arjun-XPS-13-9360 ~
nslookup -type=MX inferno.fitness
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
inferno.fitness mail exchanger = 10 aspmx2.googlemail.com.
inferno.fitness mail exchanger = 5 alt2.aspmx.l.google.com.
inferno.fitness mail exchanger = 1 aspmx.l.google.com.
inferno.fitness mail exchanger = 10 aspmx3.googlemail.com.
inferno.fitness mail exchanger = 5 alt1.aspmx.l.google.com.

Authoritative answers can be found from:
```

Observations:
This GLTD website has 5 mail servers as shown. They are all hosted by Google.

h) For www.just.jobs



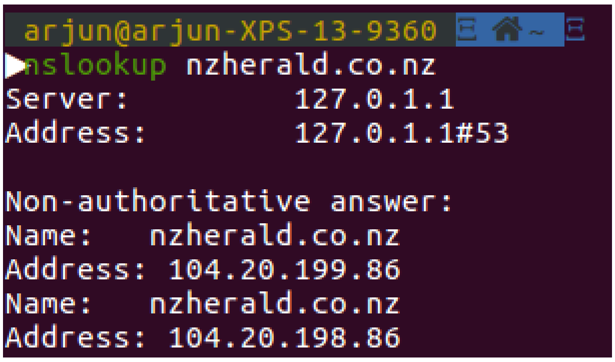
```
arjun@arjun-XPS-13-9360 ~
nslookup just.jobs
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   just.jobs
Address: 192.124.249.160
```



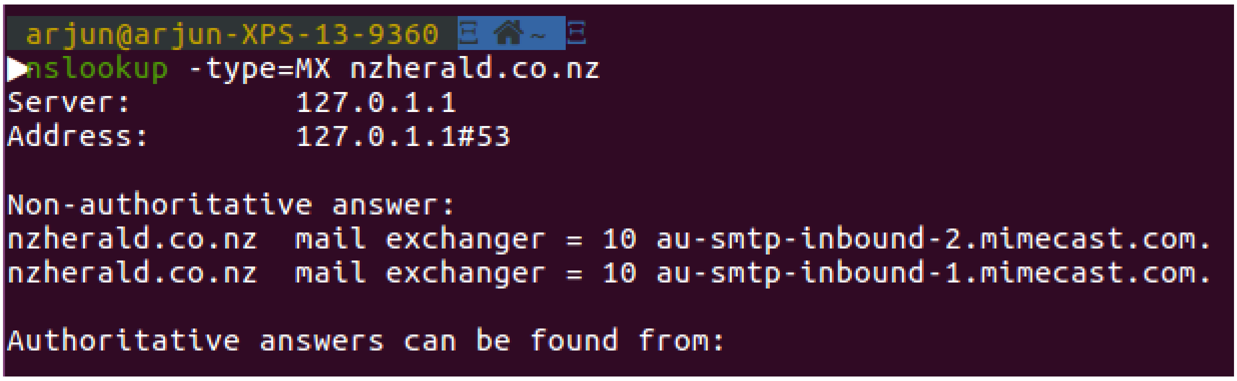
```
arjun@arjun-XPS-13-9360 ~
nslookup -type=MX just.jobs
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
just.jobs       mail exchanger = 10 alt4.aspmx.l.google.com.
just.jobs       mail exchanger = 10 alt3.aspmx.l.google.com.
just.jobs       mail exchanger = 5 alt2.aspmx.l.google.com.
just.jobs       mail exchanger = 1 aspmx.l.google.com.
just.jobs       mail exchanger = 5 alt1.aspmx.l.google.com.

Authoritative answers can be found from:
```

Observations:
This sponsored top level domain has 5 mail servers. All are hosted by Google.

i) For www.nzherald.co.nz



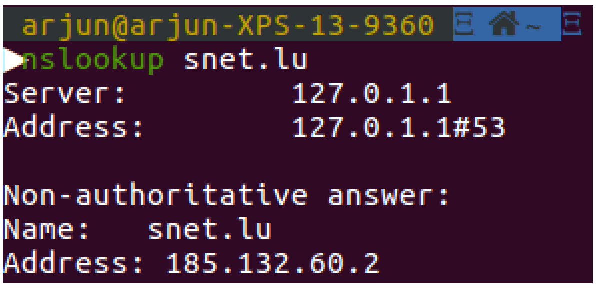
```
arjun@arjun-XPS-13-9360  ~
▶nslookup nzherald.co.nz
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   nzherald.co.nz
Address: 104.20.199.86
Name:   nzherald.co.nz
Address: 104.20.198.86
```



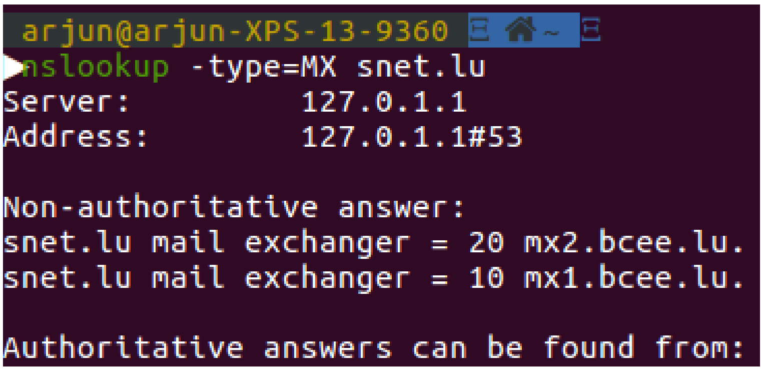
```
arjun@arjun-XPS-13-9360  ~
▶nslookup -type=MX nzherald.co.nz
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
nzherald.co.nz  mail exchanger = 10 au-smtp-inbound-2.mimecast.com.
nzherald.co.nz  mail exchanger = 10 au-smtp-inbound-1.mimecast.com.

Authoritative answers can be found from:
```

Observations:
This country level domain has 2 mail servers. Interestingly, www.indiaeducation.net also hosts its mail servers on the same website.

j) For www.snet.lu



```
arjun@arjun-XPS-13-9360  ~
▶nslookup snet.lu
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
Name:   snet.lu
Address: 185.132.60.2
```



```
arjun@arjun-XPS-13-9360  ~
▶nslookup -type=MX snet.lu
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
snet.lu mail exchanger = 20 mx2.bcee.lu.
snet.lu mail exchanger = 10 mx1.bcee.lu.

Authoritative answers can be found from:
```

Observations:
This country level domain has 2 mail servers that are both hosted in Luxembourg.

4. EXPLAINING A FEW TERMS:

We touch upon the basic definitions of some terms:

- **Serial:** The zone serial number that is incremented when the zone file is modified. Thus, the slave and secondary name servers know when the zone has been changed.
- **Refresh:** The number of seconds between update requests from secondary and slave name servers.
- **Retry:** The number of seconds the slave or secondary server will wait before retrying.
- **Expire:** The number of seconds a master or slave waits before considering the data stale if it cannot reach the primary server. This is analagous to a timeout.
- **Minimum:** This is the default TTL value specified.
- **TTL(Time To Live):** The number of seconds a domain name is cached locally before expiration and returned to authoritative name servers for updated information.

5. CONCLUSION:

From this assignment, I learnt how to analyse and understand the working of nslookup to deduce mail servers associated with a website. By filtering DNS packets from the captured packets, we get an idea of the packets transferred from our system to the domain host that sends response packets.