

# CENG 421 IP RESEARCH

Esin Sanem İMAMOĞLU

Student ID:240206006

- There are several ways to obtain IP addresses and learn about domain names but here, nslookup command is used. This command line tool provides finding IP address of a host or the domain name of an IP address. [1] In order to investigate IP address of www.yahoo.com, nslookup command is used as well. In the first line, there is an IP address of a server which computer asks for IP address of www.yahoo.com. The result is in non-authoritative answer part which are 87.248.100.216 and 87.248.100.215 as shown in Figure 1.

Next steps were analyzing mail exchanger of www.yahoo.com and IP address of it. Initially, set q=mx is typed which gives mail exchanger of the site we will type after it. There are three mail exchangers of yahoo.com. The smaller number after the equal sign has priority. But here, all of them are the same.

```
[esin@localhost ~]$ nslookup www.yahoo.com
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
www.yahoo.com    canonical name = new-fp-shed.wg1.b.yahoo.com.
Name:   new-fp-shed.wg1.b.yahoo.com
Address: 87.248.100.216
Name:   new-fp-shed.wg1.b.yahoo.com
Address: 87.248.100.215
Name:   new-fp-shed.wg1.b.yahoo.com
Address: 2a00:1288:110:c305::1:8001
Name:   new-fp-shed.wg1.b.yahoo.com
Address: 2a00:1288:110:c305::1:8000

[esin@localhost ~]$ nslookup
> set q=mx
> yahoo.com
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
yahoo.com        mail exchanger = 1 mta5.am0.yahoodns.net.
yahoo.com        mail exchanger = 1 mta6.am0.yahoodns.net.
yahoo.com        mail exchanger = 1 mta7.am0.yahoodns.net.
```

*Figure 1: IP address of www.yahoo.com*

Afterwards, “set q=a” is typed in order to switch addresses from mail exchanger. Addresses of the mail exchangers are shown in Figure 2, Figure 3 and Figure 4.

```
Authoritative answers can be found from:
> set q=a
> mta5.am0.yahoodns.net.
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
Name:   mta5.am0.yahoodns.net
Address: 67.195.204.72
Name:   mta5.am0.yahoodns.net
Address: 67.195.204.73
Name:   mta5.am0.yahoodns.net
Address: 67.195.228.109
Name:   mta5.am0.yahoodns.net
Address: 67.195.204.74
Name:   mta5.am0.yahoodns.net
Address: 98.136.96.91
Name:   mta5.am0.yahoodns.net
Address: 67.195.204.77
Name:   mta5.am0.yahoodns.net
Address: 98.136.96.75
Name:   mta5.am0.yahoodns.net
Address: 98.136.96.77
```

*Figure 2: Addresses of Mail Exchanger*

```
> mta6.am0.yahoodns.net.
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
Name:   mta6.am0.yahoodns.net
Address: 67.195.204.77
Name:   mta6.am0.yahoodns.net
Address: 98.136.96.74
Name:   mta6.am0.yahoodns.net
Address: 67.195.228.94
Name:   mta6.am0.yahoodns.net
Address: 67.195.204.72
Name:   mta6.am0.yahoodns.net
Address: 98.136.96.75
Name:   mta6.am0.yahoodns.net
Address: 98.136.96.77
Name:   mta6.am0.yahoodns.net
Address: 67.195.204.79
Name:   mta6.am0.yahoodns.net
Address: 67.195.228.106
> mta.am0.yahoodns.net.
Server:          192.168.1.1
Address:         192.168.1.1#53
```

*Figure 3: Addresses of Mail Exchanger*

```

> mta7.am0.yahoodns.net.
Server:          192.168.1.1
Address:         192.168.1.1#53

Non-authoritative answer:
Name:   mta7.am0.yahoodns.net
Address: 67.195.204.77
Name:   mta7.am0.yahoodns.net
Address: 67.195.204.72
Name:   mta7.am0.yahoodns.net
Address: 67.195.204.79
Name:   mta7.am0.yahoodns.net
Address: 67.195.228.109
Name:   mta7.am0.yahoodns.net
Address: 67.195.228.111
Name:   mta7.am0.yahoodns.net
Address: 67.195.204.74
Name:   mta7.am0.yahoodns.net
Address: 67.195.204.73
Name:   mta7.am0.yahoodns.net
Address: 98.136.96.77

```

*Figure 4: Addresses of Mail Exchanger*

- In the last part, telnet is used. Telnet is a network which provides communication via texting between two machines. Here is typed “telnet (IP number) (port number)” with blankets between them as shown in the Figure 5. In the first example, 74.53.89.587 is the IP number of www.kalfaoglu.com website. And 87.248.100.216 is the IP number of www.yahoo.com website. The reason here is used IP numbers is there occurred an unknown error when “mail.kalfaoglu.net”. [2]

```

[esin@localhost ~]$ telnet 74.53.89.82 587
Trying 74.53.89.82...
telnet: connect to address 74.53.89.82: Network is unreachable
[esin@localhost ~]$ telnet 87.248.100.216 587
Trying 87.248.100.216...
telnet: connect to address 87.248.100.216: Network is unreachable

```

*Figure 5: Sending mail using Telnet*

## Referances

- [1] «IONOS,» 13 08 2019. [Çevrimiçi]. Available: <https://www.ionos.com/digitalguide/server/tools/nslookup/>.
- [2] M. Rouse, «TechTarget,» April 2020. [Çevrimiçi]. Available: <https://searchnetworking.techtarget.com/definition/Telnet>.

