

# Exercise: Looking At DNS Response Messages and Resource Records

In this lesson, we'll use command-line tools to look at DNS response messages and resource records!

## WE'LL COVER THE FOLLOWING ^

- Revisiting **Nslookup**
  - Output
- Looking At Real DNS Response Messages With **dig**

## Revisiting **Nslookup** #

```
nslookup -type=A educative.io
```



**nslookup** is a versatile tool for DNS lookups. The **type** flag determines the type of RR that you want to look into!

## Output #

**nslookup** can be used to look at DNS records. In this example, we looked up **educative.io**.

Here's what the output may look like:

```
Server:      169.254.169.254
Address:     169.254.169.254#53
```

```
Non-authoritative answer:
```

```
Name:   educative.io
Address: 104.20.7.183
Name:   educative.io
```

- The first two lines are the IP address of the local DNS server which is `169.254.169.254` in our case.
- The last few lines return the type A RR that maps `educative.io` to the IP address `104.20.6.183`. It says ‘non-authoritative’ because the answer is coming from a local DNS server’s cache, and not from Educative’s authoritative DNS server.

If you’re wondering what `TTL` values look like, run the following command. The value in the `TTL` field is in seconds, so a value of `279` is 4 minutes and 39 seconds.

```
nslookup -debug educative.io
```



## Looking At Real DNS Response Messages With `dig` #

```
dig educative.io
```



`dig` is a command-line tool used to query DNS servers. `dig` stands for **d**omain **i**nformation **g**roper, and it displays the actual messages that were received from DNS servers. You can decipher the output for yourself now that you know what a DNS message looks like.

As always, we encourage you to read the [dig manpage](#) and explore the command for yourself!

---

We have now studied the Internet’s directory in detail. Let’s move on to another protocol. See you in the next lesson!

