ATTACK DEFENSE

by PentesterAcademy

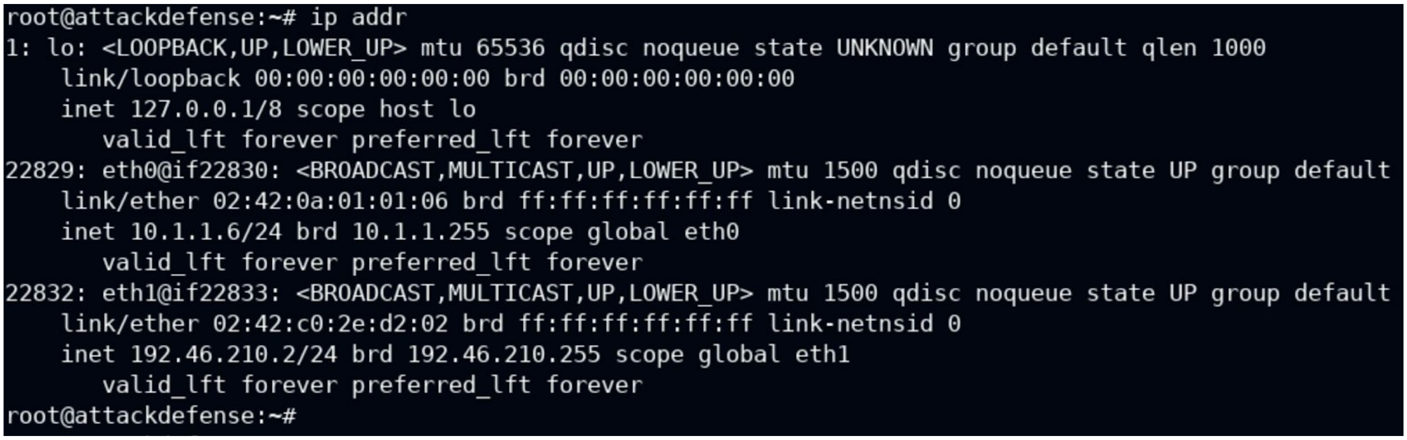
Name	NoSQL Basics
URL	https://attackdefense.com/challengedetails?cid=1803
Type	Webapp Pentesting Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

In this exercise, we will take a look at basic SQL queries this includes usage of SELECT

Identifying IP address of the target machine

Command: ip addr

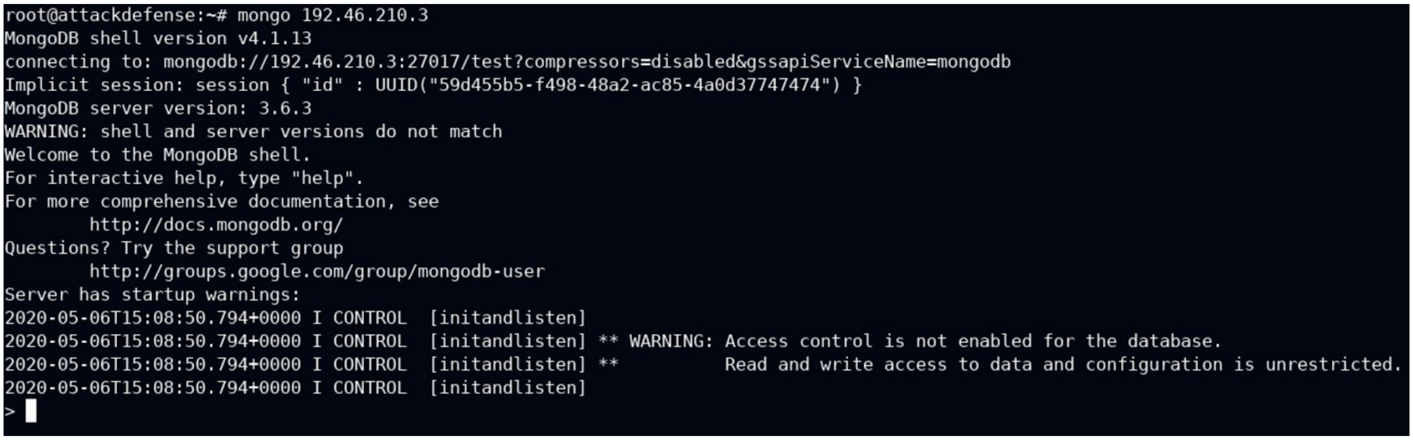


```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
22829: eth0@if22830: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:06 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.6/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
22832: eth1@if22833: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:2e:d2:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.46.210.2/24 brd 192.46.210.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.46.210.2. The target machine is located at the IP address 192.46.210.3

Step 1: Connecting to MongoDB server.

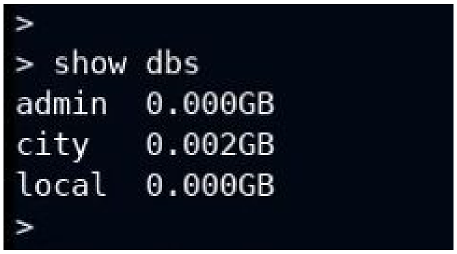
Command: mongo 192.46.210.3



```
root@attackdefense:~# mongo 192.46.210.3
MongoDB shell version v4.1.13
connecting to: mongodb://192.46.210.3:27017/test?compressors=disabled&gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("59d455b5-f498-48a2-ac85-4a0d37747474") }
MongoDB server version: 3.6.3
WARNING: shell and server versions do not match
Welcome to the MongoDB shell.
For interactive help, type "help".
For more comprehensive documentation, see
        http://docs.mongodb.org/
Questions? Try the support group
        http://groups.google.com/group/mongodb-user
Server has startup warnings:
2020-05-06T15:08:50.794+0000 I CONTROL  [initandlisten]
2020-05-06T15:08:50.794+0000 I CONTROL  [initandlisten] ** WARNING: Access control is not enabled for the database.
2020-05-06T15:08:50.794+0000 I CONTROL  [initandlisten] **          Read and write access to data and configuration is unrestricted.
2020-05-06T15:08:50.794+0000 I CONTROL  [initandlisten]
> 
```

Task 1: Listing Databases

Query: show dbs;

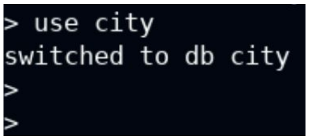


```
>
> show dbs
admin   0.000GB
city    0.002GB
local   0.000GB
>
```

There are 4 databases on the MongoDB server: admin, city, config and local. There is one user database "city". The databases "admin","config" and "local" are used by MongoDB itself.

Task 2: Selecting a database.

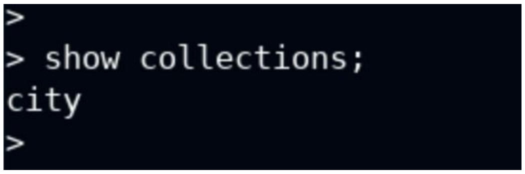
Query: use city.



```
> use city
switched to db city
>
>
```

Task 3: Listing collection stored on the "city" database.

Query: show collections

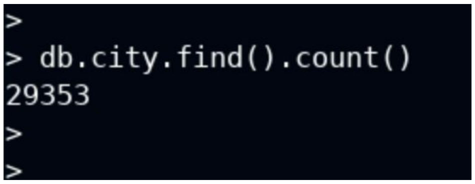


```
>
> show collections;
city
>
```

Task 4: Identifying the number of documents in the database.

Query Syntax: db.<collection-name>.find().count()

Query: db.city.find().count()

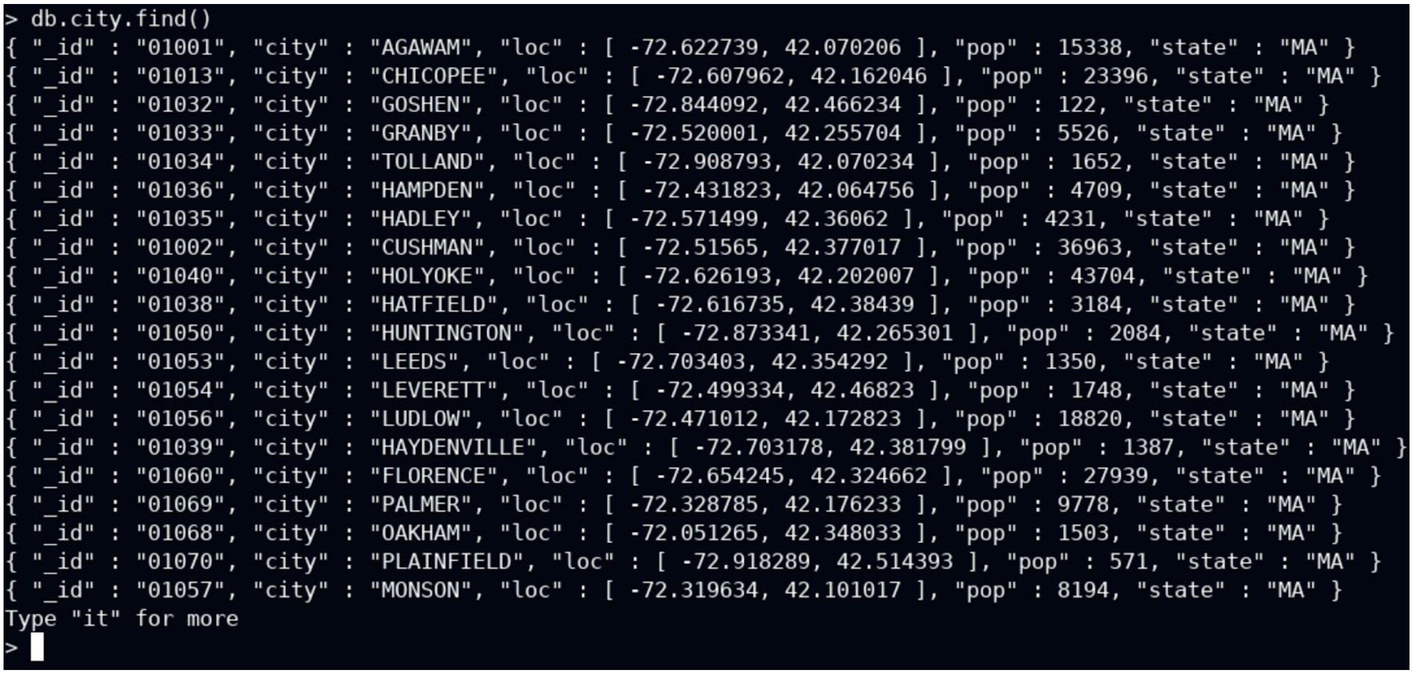


```
>
> db.city.find().count()
29353
>
>
```

There are 29353 document in the collection.

Task 5: List the documents in the city collection.

Query: db.city.find()

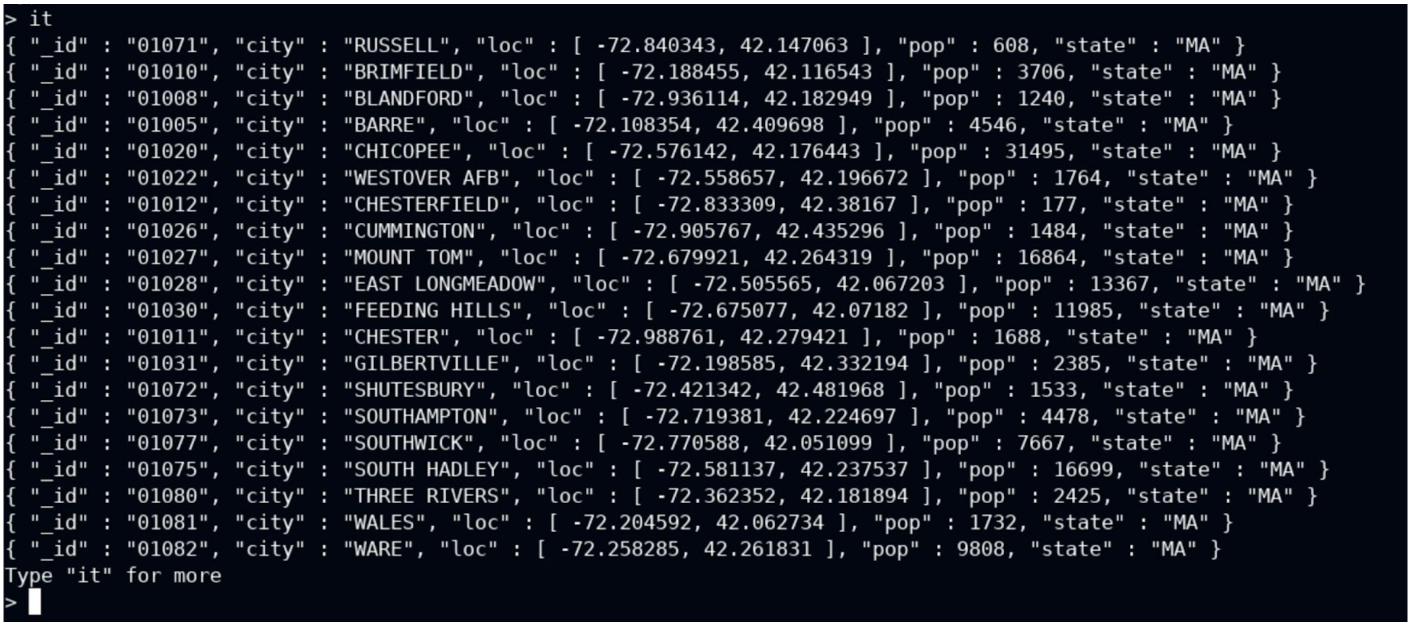


```
> db.city.find()
{ "_id" : "01001", "city" : "AGAWAM", "loc" : [ -72.622739, 42.070206 ], "pop" : 15338, "state" : "MA" }
{ "_id" : "01013", "city" : "CHICOPEE", "loc" : [ -72.607962, 42.162046 ], "pop" : 23396, "state" : "MA" }
{ "_id" : "01032", "city" : "GOSHEN", "loc" : [ -72.844092, 42.466234 ], "pop" : 122, "state" : "MA" }
{ "_id" : "01033", "city" : "GRANBY", "loc" : [ -72.520001, 42.255704 ], "pop" : 5526, "state" : "MA" }
{ "_id" : "01034", "city" : "TOLLAND", "loc" : [ -72.908793, 42.070234 ], "pop" : 1652, "state" : "MA" }
{ "_id" : "01036", "city" : "HAMPDEN", "loc" : [ -72.431823, 42.064756 ], "pop" : 4709, "state" : "MA" }
{ "_id" : "01035", "city" : "HADLEY", "loc" : [ -72.571499, 42.36062 ], "pop" : 4231, "state" : "MA" }
{ "_id" : "01002", "city" : "CUSHMAN", "loc" : [ -72.51565, 42.377017 ], "pop" : 36963, "state" : "MA" }
{ "_id" : "01040", "city" : "HOLYOKE", "loc" : [ -72.626193, 42.202007 ], "pop" : 43704, "state" : "MA" }
{ "_id" : "01038", "city" : "HATFIELD", "loc" : [ -72.616735, 42.38439 ], "pop" : 3184, "state" : "MA" }
{ "_id" : "01050", "city" : "HUNTINGTON", "loc" : [ -72.873341, 42.265301 ], "pop" : 2084, "state" : "MA" }
{ "_id" : "01053", "city" : "LEEDS", "loc" : [ -72.703403, 42.354292 ], "pop" : 1350, "state" : "MA" }
{ "_id" : "01054", "city" : "LEVERETT", "loc" : [ -72.499334, 42.46823 ], "pop" : 1748, "state" : "MA" }
{ "_id" : "01056", "city" : "LUDLOW", "loc" : [ -72.471012, 42.172823 ], "pop" : 18820, "state" : "MA" }
{ "_id" : "01039", "city" : "HAYDENVILLE", "loc" : [ -72.703178, 42.381799 ], "pop" : 1387, "state" : "MA" }
{ "_id" : "01060", "city" : "FLORENCE", "loc" : [ -72.654245, 42.324662 ], "pop" : 27939, "state" : "MA" }
{ "_id" : "01069", "city" : "PALMER", "loc" : [ -72.328785, 42.176233 ], "pop" : 9778, "state" : "MA" }
{ "_id" : "01068", "city" : "OAKHAM", "loc" : [ -72.051265, 42.348033 ], "pop" : 1503, "state" : "MA" }
{ "_id" : "01070", "city" : "PLAINFIELD", "loc" : [ -72.918289, 42.514393 ], "pop" : 571, "state" : "MA" }
{ "_id" : "01057", "city" : "MONSON", "loc" : [ -72.319634, 42.101017 ], "pop" : 8194, "state" : "MA" }
Type "it" for more
>
```

Only 20 documents of the collections are listed.

Task 6: The next 20 documents can be viewed by using "it".

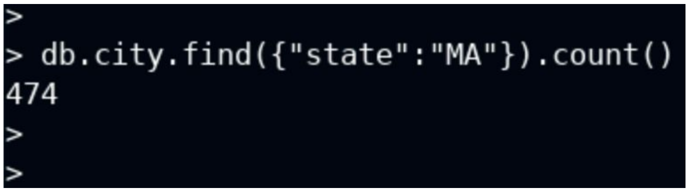
Query: it



```
> it
{ "_id" : "01071", "city" : "RUSSELL", "loc" : [ -72.840343, 42.147063 ], "pop" : 608, "state" : "MA" }
{ "_id" : "01010", "city" : "BRIMFIELD", "loc" : [ -72.188455, 42.116543 ], "pop" : 3706, "state" : "MA" }
{ "_id" : "01008", "city" : "BLANDFORD", "loc" : [ -72.936114, 42.182949 ], "pop" : 1240, "state" : "MA" }
{ "_id" : "01005", "city" : "BARRE", "loc" : [ -72.108354, 42.409698 ], "pop" : 4546, "state" : "MA" }
{ "_id" : "01020", "city" : "CHICOPEE", "loc" : [ -72.576142, 42.176443 ], "pop" : 31495, "state" : "MA" }
{ "_id" : "01022", "city" : "WESTOVER AFB", "loc" : [ -72.558657, 42.196672 ], "pop" : 1764, "state" : "MA" }
{ "_id" : "01012", "city" : "CHESTERFIELD", "loc" : [ -72.833309, 42.38167 ], "pop" : 177, "state" : "MA" }
{ "_id" : "01026", "city" : "CUMMINGTON", "loc" : [ -72.905767, 42.435296 ], "pop" : 1484, "state" : "MA" }
{ "_id" : "01027", "city" : "MOUNT TOM", "loc" : [ -72.679921, 42.264319 ], "pop" : 16864, "state" : "MA" }
{ "_id" : "01028", "city" : "EAST LONGMEADOW", "loc" : [ -72.505565, 42.067203 ], "pop" : 13367, "state" : "MA" }
{ "_id" : "01030", "city" : "FEEDING HILLS", "loc" : [ -72.675077, 42.07182 ], "pop" : 11985, "state" : "MA" }
{ "_id" : "01011", "city" : "CHESTER", "loc" : [ -72.988761, 42.279421 ], "pop" : 1688, "state" : "MA" }
{ "_id" : "01031", "city" : "GILBERTVILLE", "loc" : [ -72.198585, 42.332194 ], "pop" : 2385, "state" : "MA" }
{ "_id" : "01072", "city" : "SHUTESBURY", "loc" : [ -72.421342, 42.481968 ], "pop" : 1533, "state" : "MA" }
{ "_id" : "01073", "city" : "SOUTHAMPTON", "loc" : [ -72.719381, 42.224697 ], "pop" : 4478, "state" : "MA" }
{ "_id" : "01077", "city" : "SOUTHWICK", "loc" : [ -72.770588, 42.051099 ], "pop" : 7667, "state" : "MA" }
{ "_id" : "01075", "city" : "SOUTH HADLEY", "loc" : [ -72.581137, 42.237537 ], "pop" : 16699, "state" : "MA" }
{ "_id" : "01080", "city" : "THREE RIVERS", "loc" : [ -72.362352, 42.181894 ], "pop" : 2425, "state" : "MA" }
{ "_id" : "01081", "city" : "WALES", "loc" : [ -72.204592, 42.062734 ], "pop" : 1732, "state" : "MA" }
{ "_id" : "01082", "city" : "WARE", "loc" : [ -72.258285, 42.261831 ], "pop" : 9808, "state" : "MA" }
Type "it" for more
>
```

Task 7: Searching for documents with specific property. Identifying the cities which belong to the state "MA".

Query: db.city.find({"state":"MA"}).count()

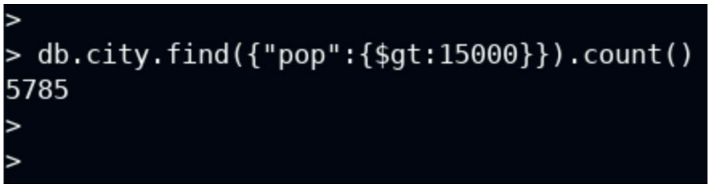


```
>
> db.city.find({"state":"MA"}).count()
474
>
>
```

There were 474 cities in the database.

Task 8: Using Greater than operation on a property. Identifying the number of cities which have populations greater than 15000.

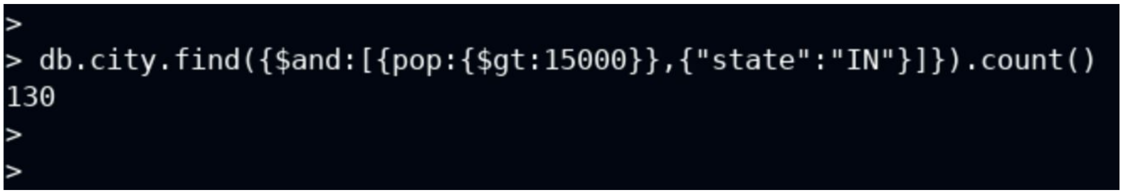
Query: db.city.find({"pop":{$gt:15000}}).count()



```
>
> db.city.find({"pop":{$gt:15000}}).count()
5785
>
>
```

Task 9: Using multiple conditions with AND operator. Identify the number of cities which population is greater than 15000 in the state of Indiana.

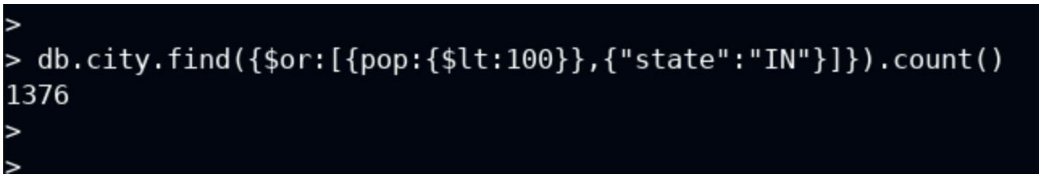
Query: db.city.find({$and:[{pop:{$gt:15000}},{"state":"IN"}]}).count()



```
>
> db.city.find({$and:[{pop:{$gt:15000}},{"state":"IN"}]}).count()
130
>
>
```

Task 10: Using multiple conditions with OR operator. Identify the number of cities which have population less than 100 or are in the state of Indiana.

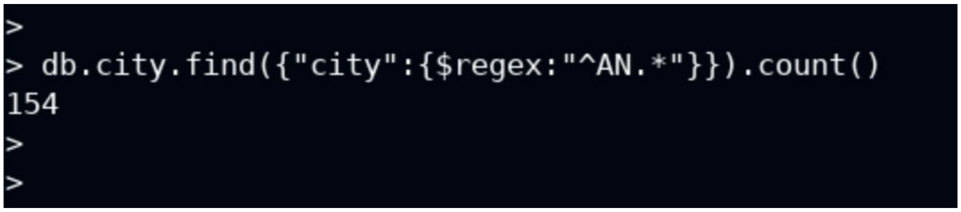
Query: db.city.find({$or:[{pop:{$lt:100}},{"state":"IN"}]}).count()



```
>
> db.city.find({$or:[{pop:{$lt:100}},{"state":"IN"}]}).count()
1376
>
>
```

Task 11: Using regex to filter documents. Identify the number of cities which start with "AN".

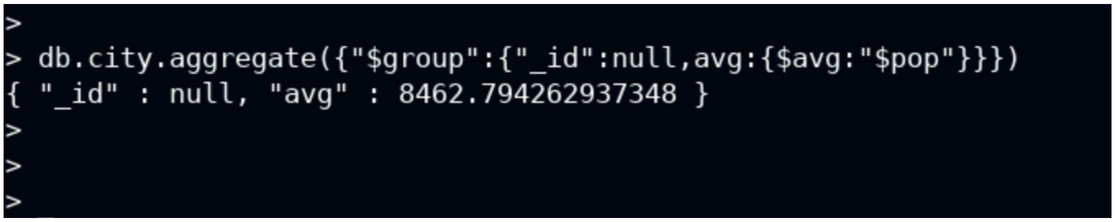
Query: db.city.find({"city":{$regex:"^AN.*"}}).count()



```
>
> db.city.find({"city":{$regex:"^AN.*"}}).count()
154
>
>
```

Task 12: Using aggregation methods. Calculate the average population.

Query: db.city.aggregate({"$group":{"_id":null,avg:{$avg:"$pop"}}})



```
>
> db.city.aggregate({"$group":{"_id":null,avg:{$avg:"$pop"}}})
{ "_id" : null, "avg" : 8462.794262937348 }
>
>
>
```

References:

1. MongoDB (https://www.mongodb.com/)
2. mongo (https://docs.mongodb.com/manual/mongo/)