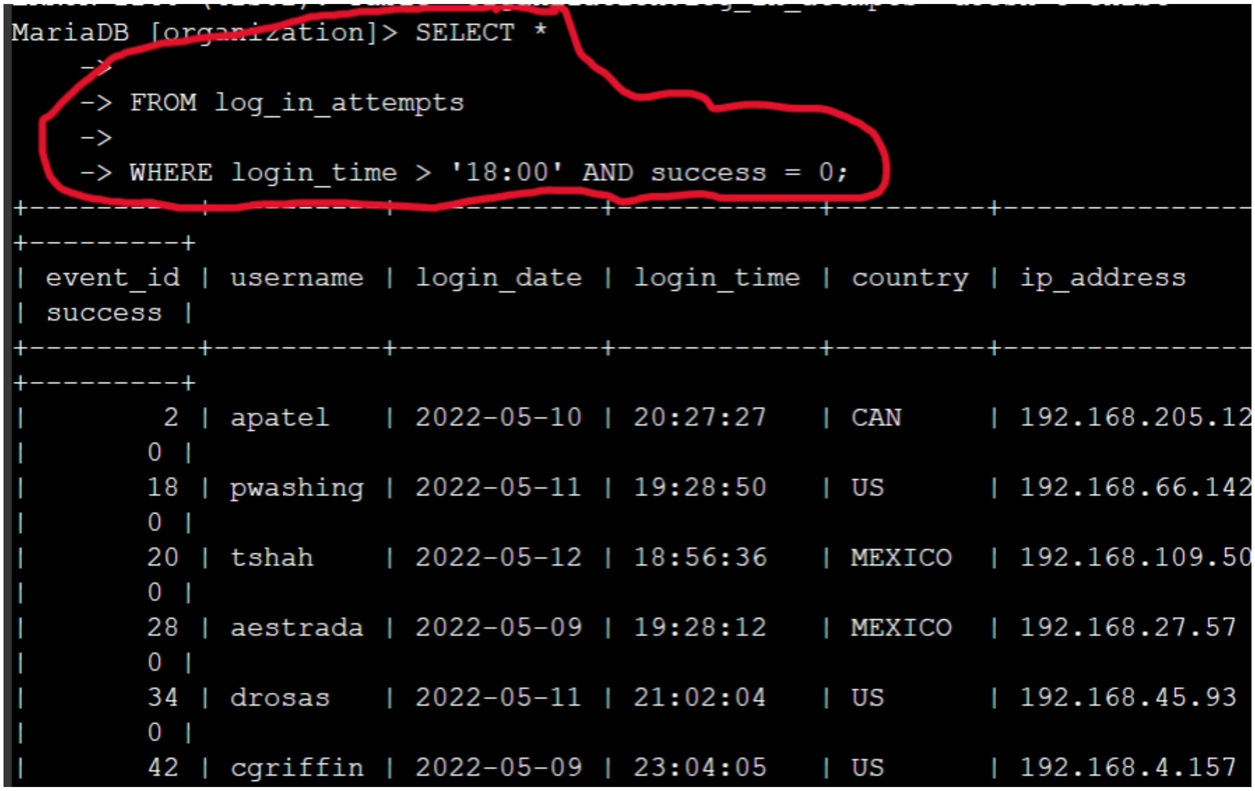
Apply filters to SQL queries

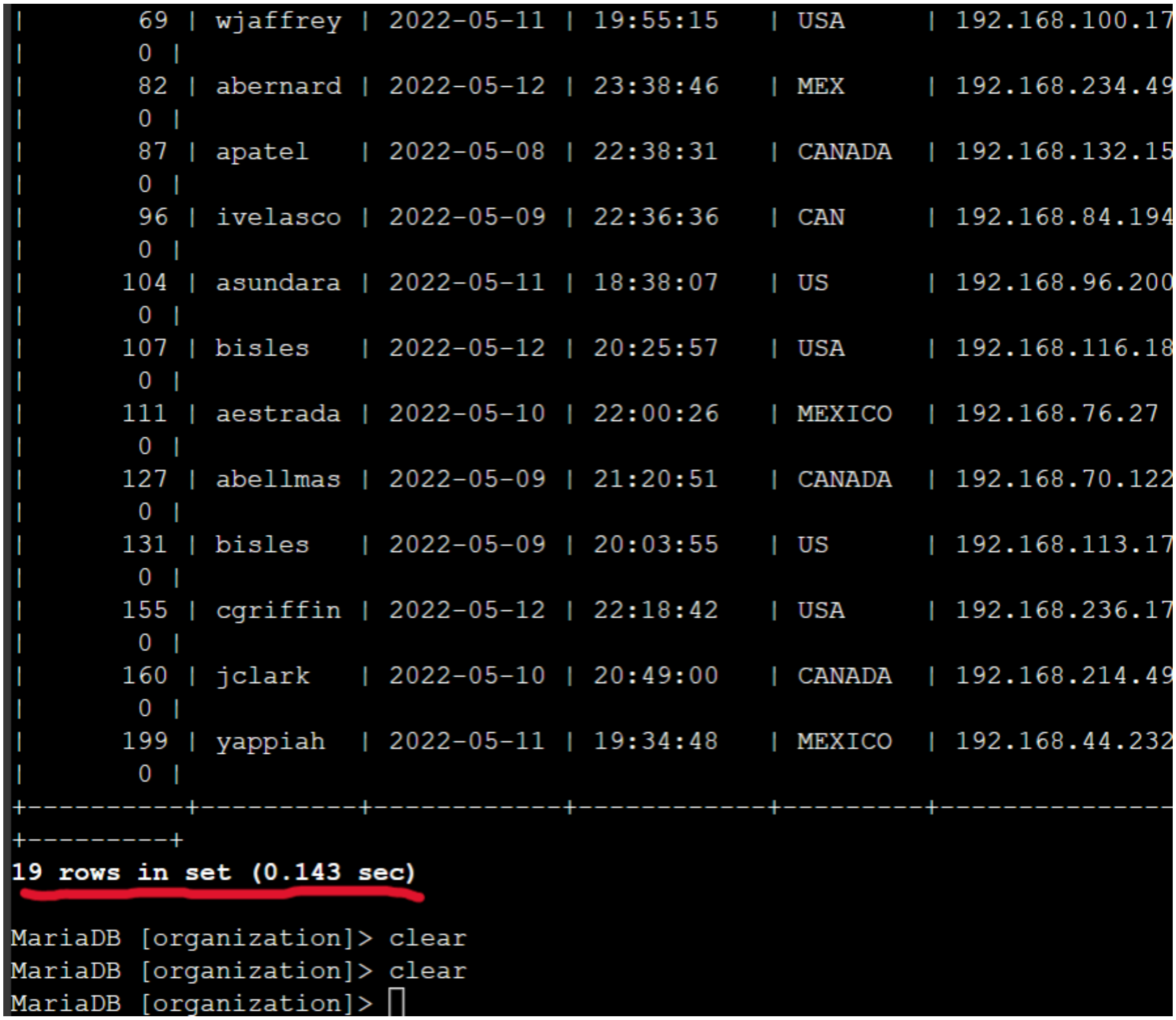
Project description

Applied SQL queries to search specific content/information. I also applied filters to help focus my search through the data base to make my hunt for info less time consuming and more precise

Retrieve after hours failed login attempts

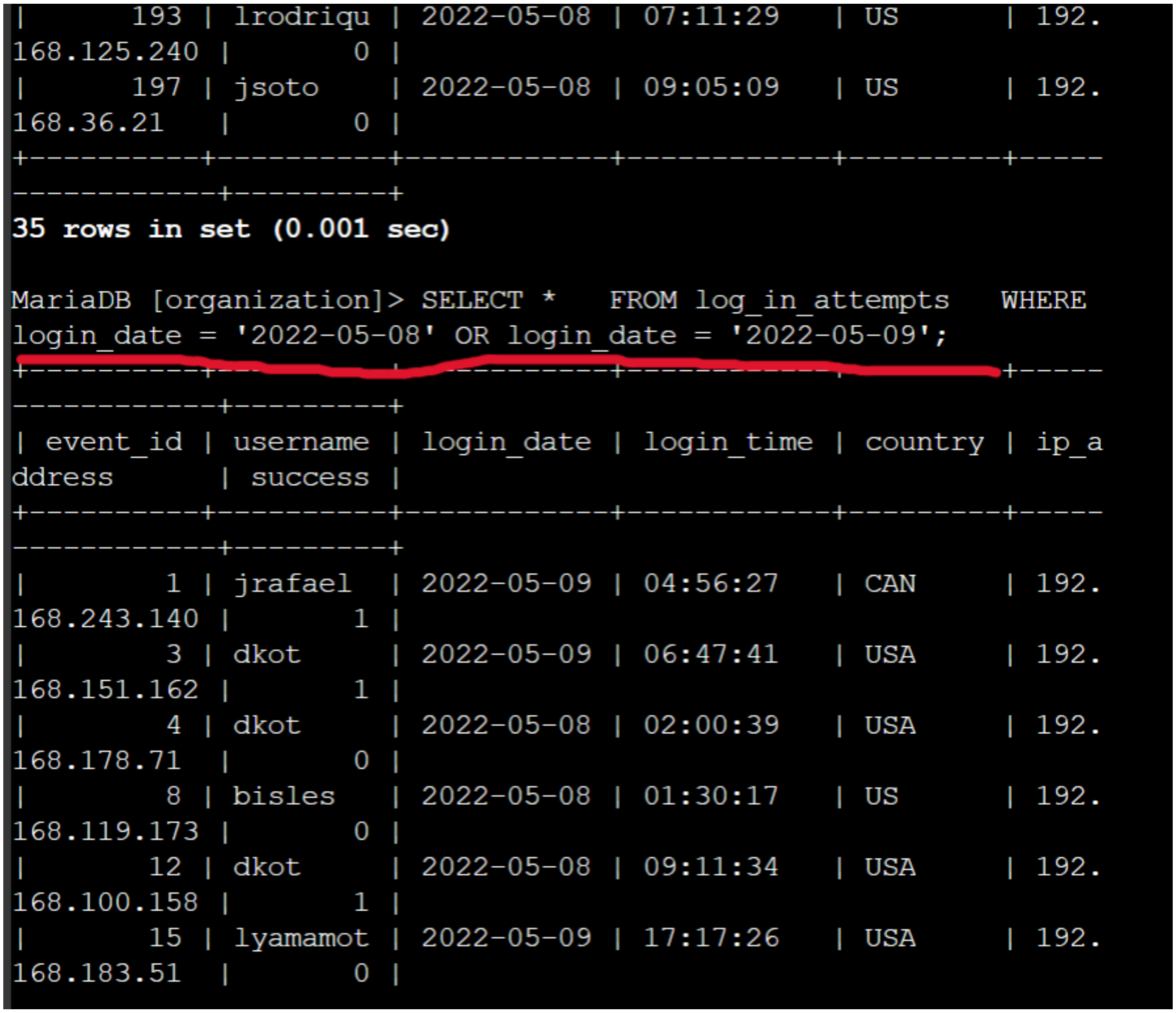


```
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE login_time > '18:00' AND success = 0;
+----------+----------+------------+------------+---------+--------------
+---------+
| event_id | username | login_date | login_time | country | ip_address
| success |
+----------+----------+------------+------------+---------+--------------
+---------+
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.205.12
|       0 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.142
|       0 |
|       20 | tshah    | 2022-05-12 | 18:56:36   | MEXICO  | 192.168.109.50
|       0 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.57
|       0 |
|       34 | drosas   | 2022-05-11 | 21:02:04   | US      | 192.168.45.93
|       0 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.157
```

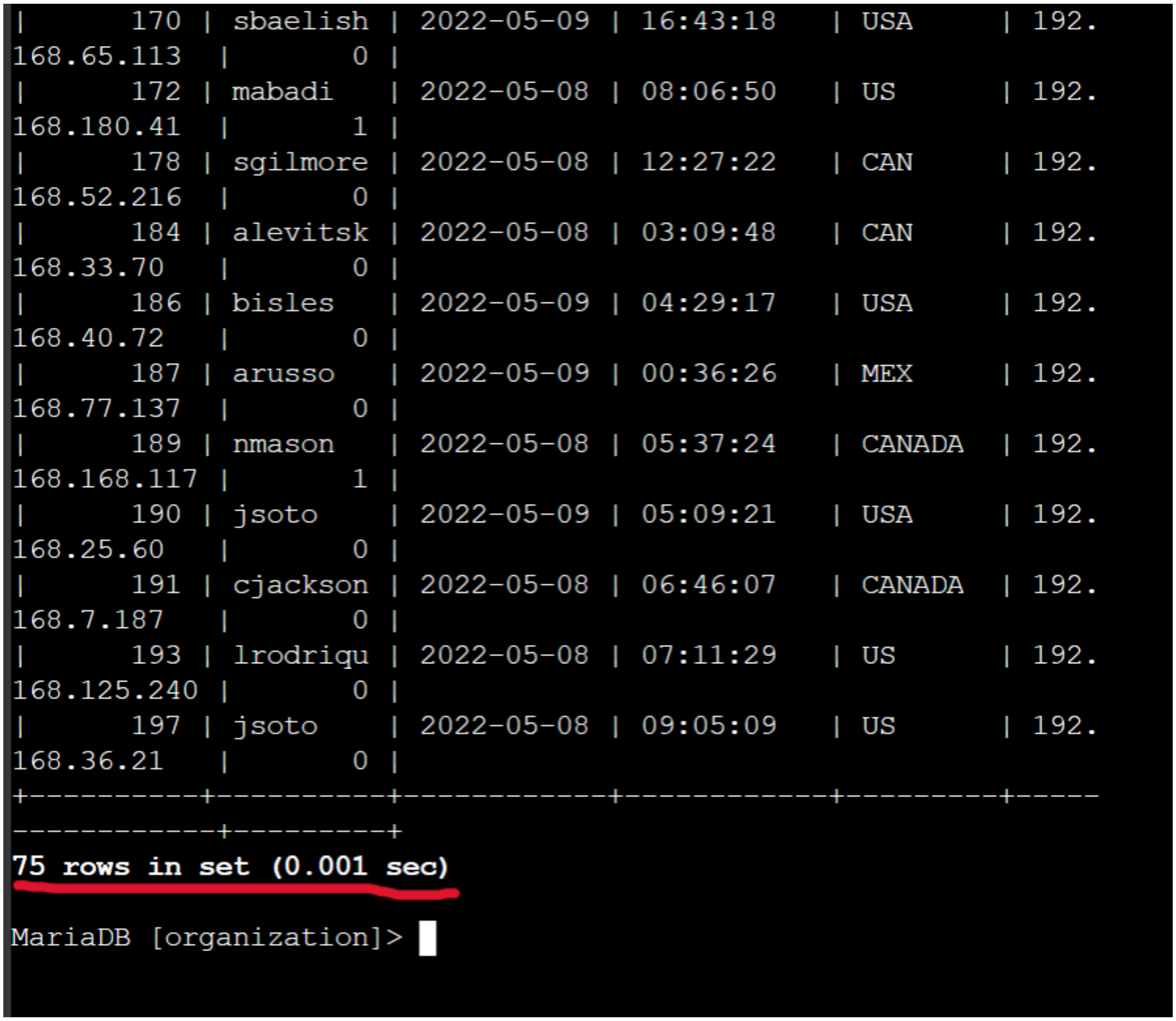


```
|       69 | wjaffrey | 2022-05-11 | 19:55:15   | USA     | 192.168.100.17
|       0 |
|       82 | abernard | 2022-05-12 | 23:38:46   | MEX     | 192.168.234.49
|       0 |
|       87 | apatel   | 2022-05-08 | 22:38:31   | CANADA  | 192.168.132.15
|       0 |
|       96 | ivelasco | 2022-05-09 | 22:36:36   | CAN     | 192.168.84.194
|       0 |
|      104 | asundara | 2022-05-11 | 18:38:07   | US      | 192.168.96.200
|       0 |
|      107 | bisles   | 2022-05-12 | 20:25:57   | USA     | 192.168.116.18
|       0 |
|      111 | aestrada | 2022-05-10 | 22:00:26   | MEXICO  | 192.168.76.27
|       0 |
|      127 | abellmas | 2022-05-09 | 21:20:51   | CANADA  | 192.168.70.122
|       0 |
|      131 | bisles   | 2022-05-09 | 20:03:55   | US      | 192.168.113.17
|       0 |
|      155 | cgriffin | 2022-05-12 | 22:18:42   | USA     | 192.168.236.17
|       0 |
|      160 | jclark   | 2022-05-10 | 20:49:00   | CANADA  | 192.168.214.49
|       0 |
|      199 | yappiah  | 2022-05-11 | 19:34:48   | MEXICO  | 192.168.44.232
|       0 |
+----------+----------+------------+------------+---------+--------------
+---------+
19 rows in set (0.143 sec)

MariaDB [organization]> clear
MariaDB [organization]> clear
MariaDB [organization]> 
```

Retrieve login attempts on specific dates

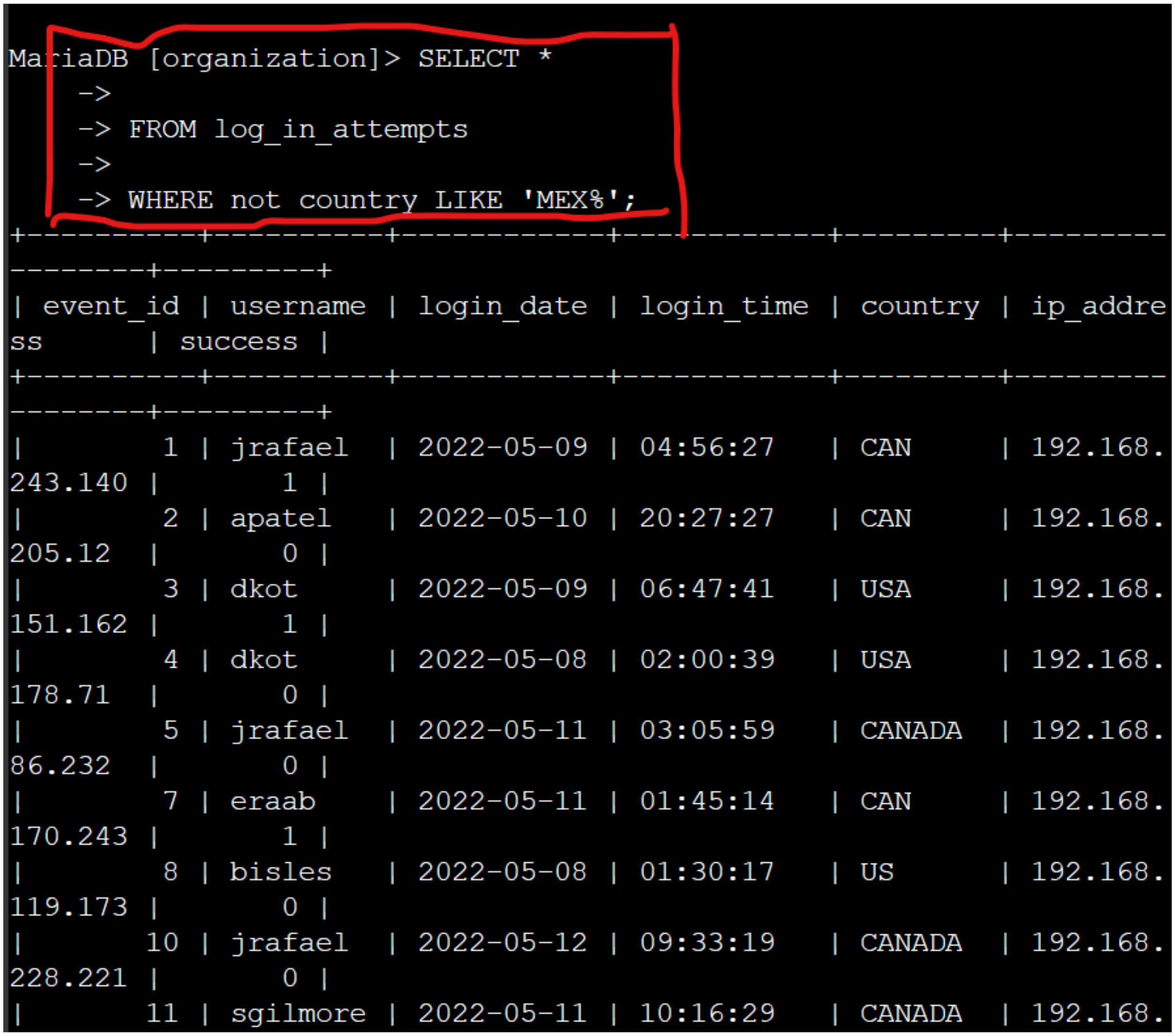


```
|       193 | lrodriqu | 2022-05-08 | 07:11:29   | US       | 192.
168.125.240 |       0 |
|       197 | jsoto    | 2022-05-08 | 09:05:09   | US       | 192.
168.36.21   |       0 |
+-----------+----------+------------+------------+---------+-----
------------+---------+
35 rows in set (0.001 sec)

MariaDB [organization]> SELECT *   FROM log_in_attempts   WHERE
login_date = '2022-05-08' OR login_date = '2022-05-09';
+-----------+----------+------------+------------+---------+-----
------------+---------+
| event_id | username | login_date | login_time | country | ip_a
ddress      | success |
+-----------+----------+------------+------------+---------+-----
------------+---------+
|         1 | jrafael  | 2022-05-09 | 04:56:27   | CAN      | 192.
168.243.140 |       1 |
|         3 | dkot     | 2022-05-09 | 06:47:41   | USA      | 192.
168.151.162 |       1 |
|         4 | dkot     | 2022-05-08 | 02:00:39   | USA      | 192.
168.178.71  |       0 |
|         8 | bisles   | 2022-05-08 | 01:30:17   | US       | 192.
168.119.173 |       0 |
|        12 | dkot     | 2022-05-08 | 09:11:34   | USA      | 192.
168.100.158 |       1 |
|        15 | lyamamot | 2022-05-09 | 17:17:26   | USA      | 192.
168.183.51  |       0 |
```

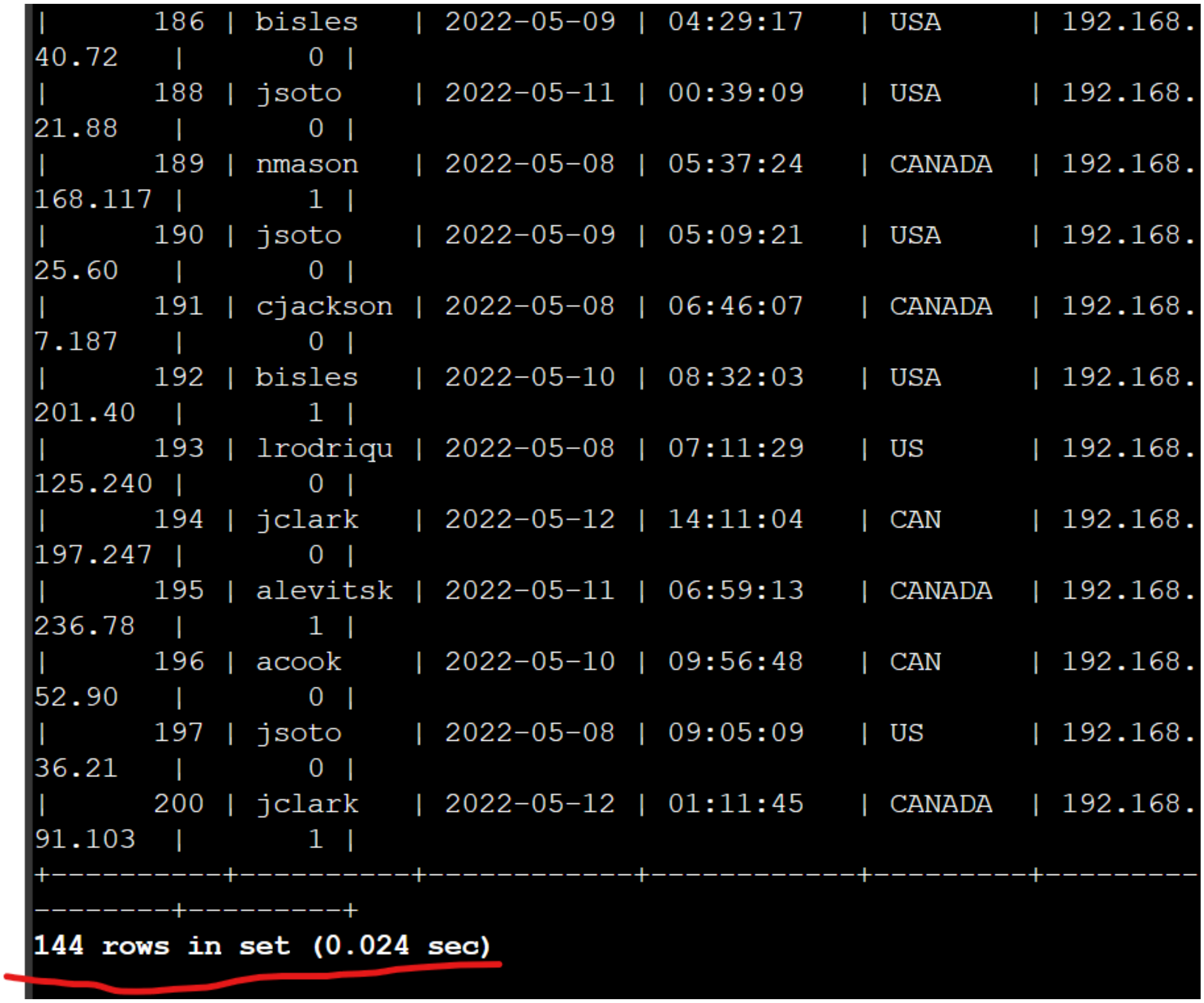


```
|       170 | sbaelish | 2022-05-09 | 16:43:18   | USA     | 192.
168.65.113  |        0 |
|       172 | mabadi   | 2022-05-08 | 08:06:50   | US      | 192.
168.180.41  |        1 |
|       178 | sgilmore | 2022-05-08 | 12:27:22   | CAN     | 192.
168.52.216  |        0 |
|       184 | alevitsk | 2022-05-08 | 03:09:48   | CAN     | 192.
168.33.70   |        0 |
|       186 | bisles   | 2022-05-09 | 04:29:17   | USA     | 192.
168.40.72   |        0 |
|       187 | arusso   | 2022-05-09 | 00:36:26   | MEX     | 192.
168.77.137  |        0 |
|       189 | nmason   | 2022-05-08 | 05:37:24   | CANADA  | 192.
168.168.117 |        1 |
|       190 | jsoto    | 2022-05-09 | 05:09:21   | USA     | 192.
168.25.60   |        0 |
|       191 | cjackson | 2022-05-08 | 06:46:07   | CANADA  | 192.
168.7.187   |        0 |
|       193 | lrodriqu | 2022-05-08 | 07:11:29   | US      | 192.
168.125.240 |        0 |
|       197 | jsoto    | 2022-05-08 | 09:05:09   | US      | 192.
168.36.21   |        0 |
+-----------+----------+------------+------------+---------+-----
------------+----------+
75 rows in set (0.001 sec)

MariaDB [organization]> █
```

Retrieve login attempts outside of Mexico

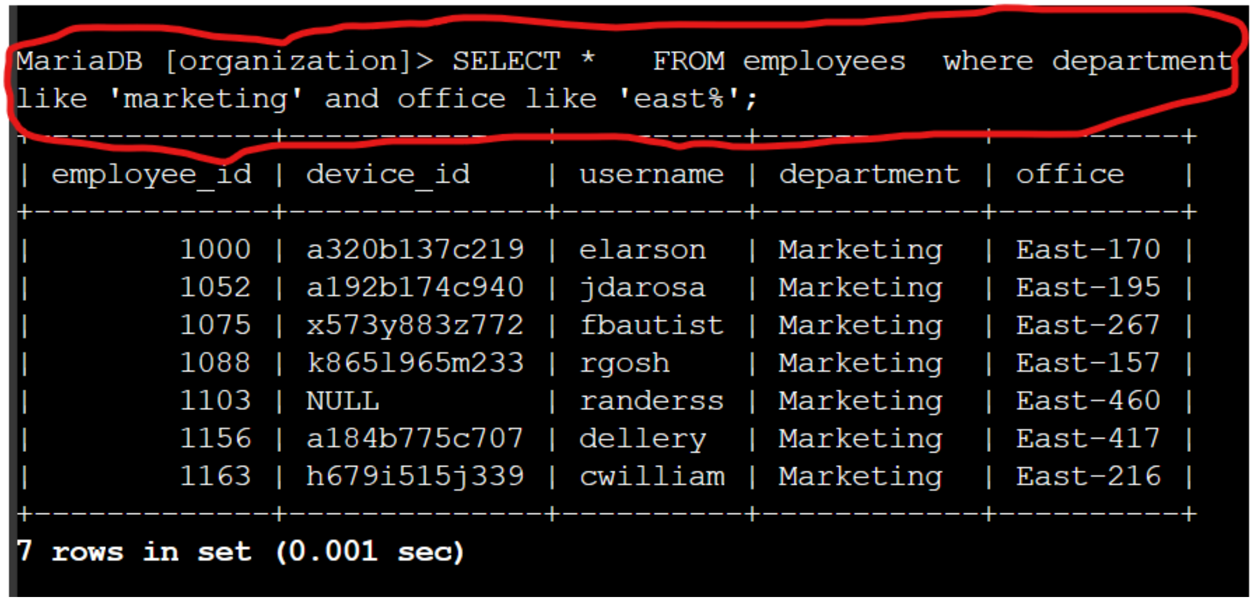


```
MariaDB [organization]> SELECT *
    ->
    -> FROM log_in_attempts
    ->
    -> WHERE not country LIKE 'MEX%';
+----------+----------+------------+------------+---------+---------
---------+---------+
| event_id | username | login_date | login_time | country | ip_addre
ss       | success |
+----------+----------+------------+------------+---------+---------
---------+---------+
|        1 | jrafael  | 2022-05-09 | 04:56:27   | CAN     | 192.168.
243.140 |       1 |
|        2 | apatel   | 2022-05-10 | 20:27:27   | CAN     | 192.168.
205.12  |       0 |
|        3 | dkot     | 2022-05-09 | 06:47:41   | USA     | 192.168.
151.162 |       1 |
|        4 | dkot     | 2022-05-08 | 02:00:39   | USA     | 192.168.
178.71  |       0 |
|        5 | jrafael  | 2022-05-11 | 03:05:59   | CANADA  | 192.168.
86.232  |       0 |
|        7 | eraab    | 2022-05-11 | 01:45:14   | CAN     | 192.168.
170.243 |       1 |
|        8 | bisles   | 2022-05-08 | 01:30:17   | US      | 192.168.
119.173 |       0 |
|       10 | jrafael  | 2022-05-12 | 09:33:19   | CANADA  | 192.168.
228.221 |       0 |
|       11 | sgilmore | 2022-05-11 | 10:16:29   | CANADA  | 192.168.
```



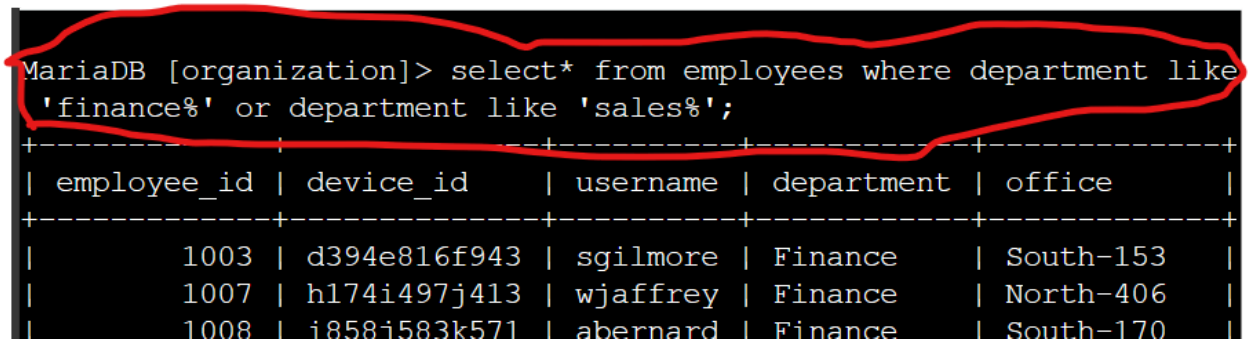
```
|       186 | bisles   | 2022-05-09 | 04:29:17   | USA     | 192.168.
40.72   |        0 |
|       188 | jsoto    | 2022-05-11 | 00:39:09   | USA     | 192.168.
21.88   |        0 |
|       189 | nmason   | 2022-05-08 | 05:37:24   | CANADA  | 192.168.
168.117 |        1 |
|       190 | jsoto    | 2022-05-09 | 05:09:21   | USA     | 192.168.
25.60   |        0 |
|       191 | cjackson | 2022-05-08 | 06:46:07   | CANADA  | 192.168.
7.187   |        0 |
|       192 | bisles   | 2022-05-10 | 08:32:03   | USA     | 192.168.
201.40  |        1 |
|       193 | lrodriqu | 2022-05-08 | 07:11:29   | US      | 192.168.
125.240 |        0 |
|       194 | jclark   | 2022-05-12 | 14:11:04   | CAN     | 192.168.
197.247 |        0 |
|       195 | alevitsk | 2022-05-11 | 06:59:13   | CANADA  | 192.168.
236.78  |        1 |
|       196 | acook    | 2022-05-10 | 09:56:48   | CAN     | 192.168.
52.90   |        0 |
|       197 | jsoto    | 2022-05-08 | 09:05:09   | US      | 192.168.
36.21   |        0 |
|       200 | jclark   | 2022-05-12 | 01:11:45   | CANADA  | 192.168.
91.103  |        1 |
+----------+----------+------------+------------+---------+---------
--------+---------+
144 rows in set (0.024 sec)
```

Retrieve employees in Marketing



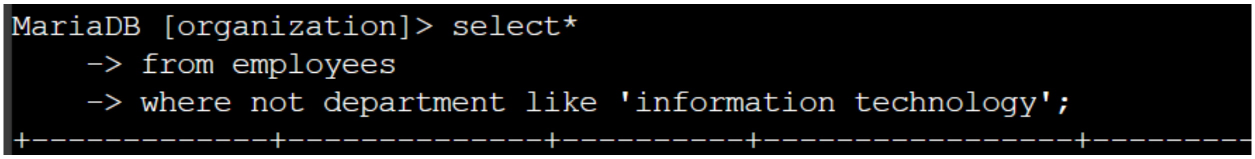
```
MariaDB [organization]> SELECT *   FROM employees  where department
like 'marketing' and office like 'east%';
+-------------+--------------+----------+------------+-----------+
| employee_id | device_id    | username | department | office    |
+-------------+--------------+----------+------------+-----------+
|        1000 | a320b137c219 | elarson  | Marketing  | East-170  |
|        1052 | a192b174c940 | jdarosa  | Marketing  | East-195  |
|        1075 | x573y883z772 | fbautist | Marketing  | East-267  |
|        1088 | k8651965m233 | rgosh    | Marketing  | East-157  |
|        1103 | NULL         | randerss | Marketing  | East-460  |
|        1156 | a184b775c707 | dellery  | Marketing  | East-417  |
|        1163 | h679i515j339 | cwilliam | Marketing  | East-216  |
+-------------+--------------+----------+------------+-----------+
7 rows in set (0.001 sec)
```

Retrieve employees in Finance or Sales

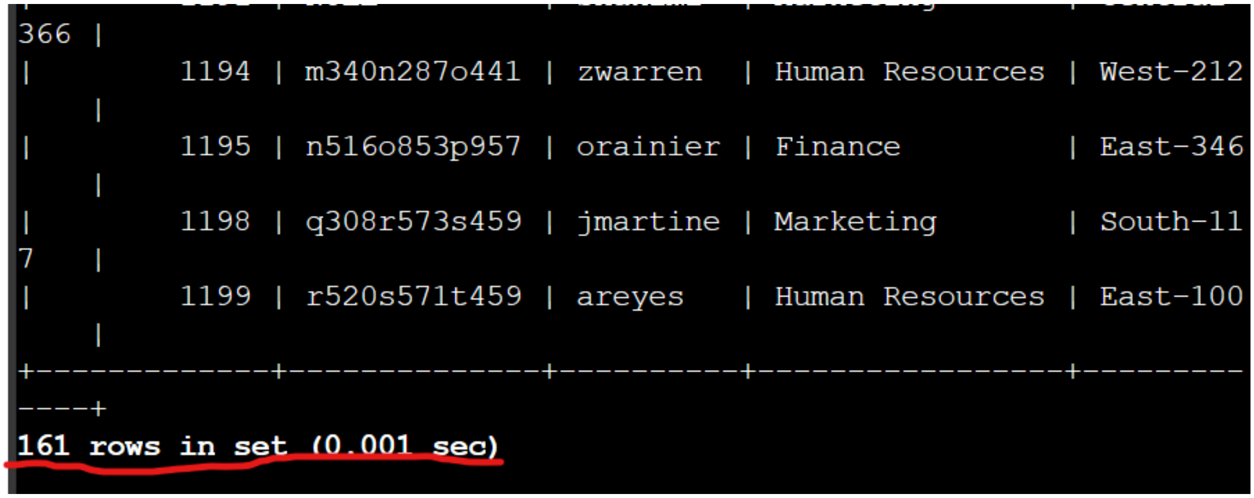


```
MariaDB [organization]> select* from employees where department like
 'finance%' or department like 'sales%';
+-------------+--------------+----------+------------+-------------+
| employee_id | device_id    | username | department | office      |
+-------------+--------------+----------+------------+-------------+
|        1003 | d394e816f943 | sgilmore | Finance    | South-153   |
|        1007 | h174i497j413 | wjaffrey | Finance    | North-406   |
|        1008 | i858j583k571 | abernard | Finance    | South-170   |
```

Retrieve all employees not in IT



```
MariaDB [organization]> select*
    -> from employees
    -> where not department like 'information technology';
+-------------+--------------+----------+-----------------+---------
```



```
366 |
|         1194 | m340n287o441 | zwarren  | Human Resources | West-212
    |
|         1195 | n516o853p957 | orainier | Finance         | East-346
    |
|         1198 | q308r573s459 | jmartine | Marketing       | South-11
7   |
|         1199 | r520s571t459 | areyes   | Human Resources | East-100
    |
+-------------+--------------+----------+-----------------+---------
----+
161 rows in set (0.001 sec)
```

Summary

SQL Queries are used to retrieve data from off/on premises databases/servers. This allows Security professionals to collect company or customer data and ensure the availability and integrity of logs and system information. Also applying filters to SQL queries allows sec professionals to quickly locate precise data/info if need be. Which, as a result, saves time and relieves the stress of sifting through unrelated data to find exactly what you are looking for.