Apply filters to SQL queries

Project description

You are a security professional at a large organization. Part of your job is to investigate security issues to help keep the system secure. You recently discovered some potential security issues that involve login attempts and employee machines.

Your task is to examine the organization's data in their *employees* and *log_in_attempts* tables. You'll need to use SQL filters to retrieve records from different datasets and investigate the potential security issues.

Task 1. Retrieve after hours failed login attempts

My team is investigating failed login attempts that were made after business hours. I want to retrieve this information from the login activity. I'll identify all unsuccessful attempts after 18:00.

Task 2. Retrieve login attempts on specific dates

My team is investigating a suspicious event that occurred on `'2022-05-09'`. I want to retrieve all login attempts that occurred on this day and the day before (`'2022-05-08'`).

Task 3. Retrieve login attempts outside of Mexico

My team is investigating logins that did not originate in Mexico, and I need to find this information. Note that the country field includes entries with `'MEX'` and `'MEXICO'`. I should use the `NOT` and `LIKE` operators and the matching pattern `'MEX%'`.

Task 4. Retrieve employees in Marketing

I need to retrieve the information from the `department` and `office` columns in the `employees` table.

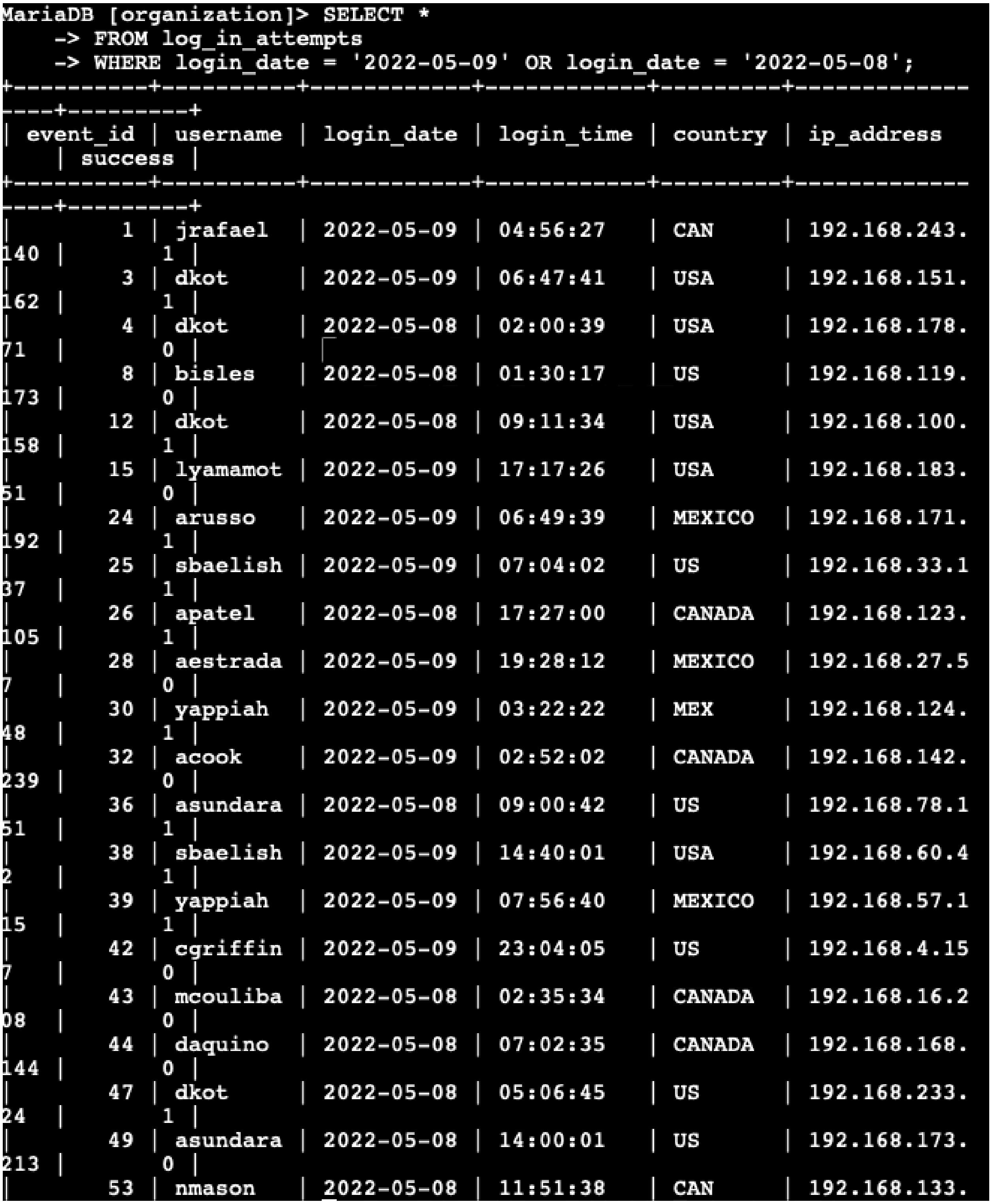
Task 5. Retrieve employees in Finance or Sales

My team needs to perform a different update to the computers of all employees in the Finance or the Sales department, and I need to locate information on these employees.

Task 6. Retrieve all employees not in IT

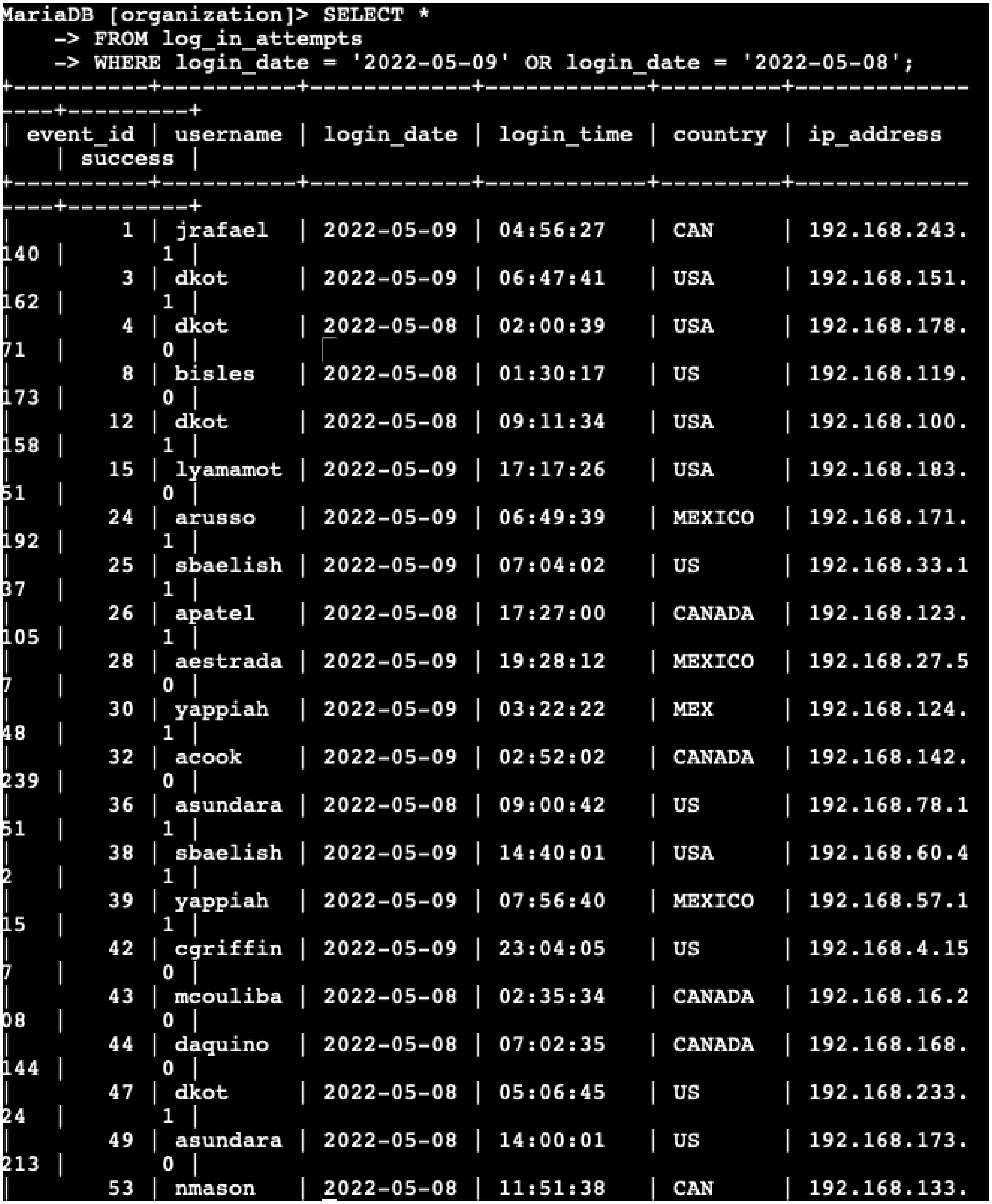
My team needs to make one more update. This update was already made to employee computers in the Information Technology department. The team needs information about employees who are not in that department. I should use the `NOT` operator to identify these employees.

Retrieve after hours failed login attempts



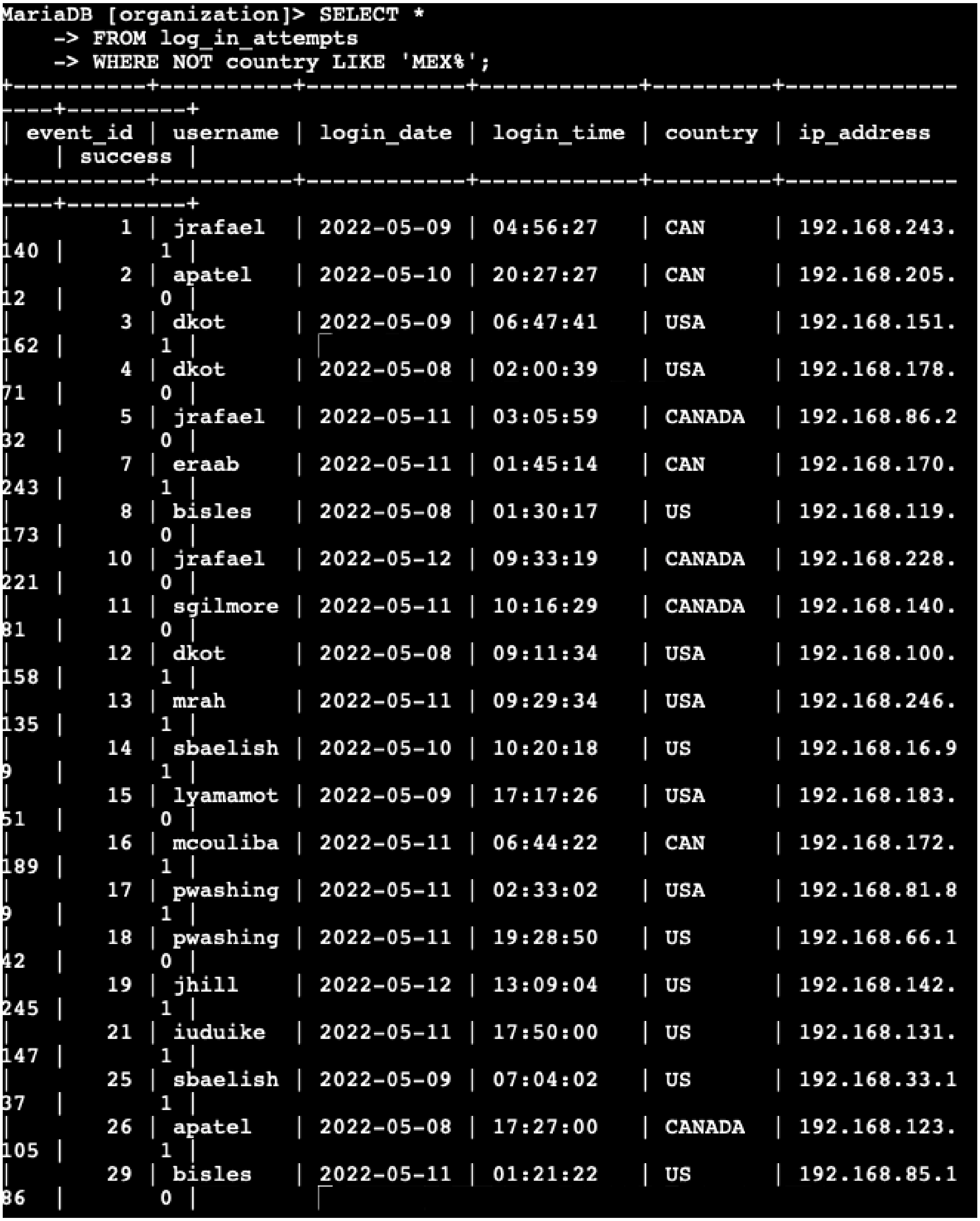
```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
+----------+----------+------------+------------+---------+------------
----+---------+
| event_id | username | login_date | login_time | country | ip_address
    | success |
+----------+----------+------------+------------+---------+------------
----+---------+
|        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 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.
192 |       1 |
|       25 | sbaelish | 2022-05-09 | 07:04:02   | US      | 192.168.33.1
37  |       1 |
|       26 | apatel   | 2022-05-08 | 17:27:00   | CANADA  | 192.168.123.
105 |       1 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.5
7   |       0 |
|       30 | yappiah  | 2022-05-09 | 03:22:22   | MEX     | 192.168.124.
48  |       1 |
|       32 | acook    | 2022-05-09 | 02:52:02   | CANADA  | 192.168.142.
239 |       0 |
|       36 | asundara | 2022-05-08 | 09:00:42   | US      | 192.168.78.1
51  |       1 |
|       38 | sbaelish | 2022-05-09 | 14:40:01   | USA     | 192.168.60.4
2   |       1 |
|       39 | yappiah  | 2022-05-09 | 07:56:40   | MEXICO  | 192.168.57.1
15  |       1 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.15
7   |       0 |
|       43 | mcouliba | 2022-05-08 | 02:35:34   | CANADA  | 192.168.16.2
08  |       0 |
|       44 | daquino  | 2022-05-08 | 07:02:35   | CANADA  | 192.168.168.
144 |       0 |
|       47 | dkot     | 2022-05-08 | 05:06:45   | US      | 192.168.233.
24  |       1 |
|       49 | asundara | 2022-05-08 | 14:00:01   | US      | 192.168.173.
213 |       0 |
|       53 | nmason   | 2022-05-08 | 11:51:38   | CAN     | 192.168.133.
```

Retrieve login attempts on specific dates



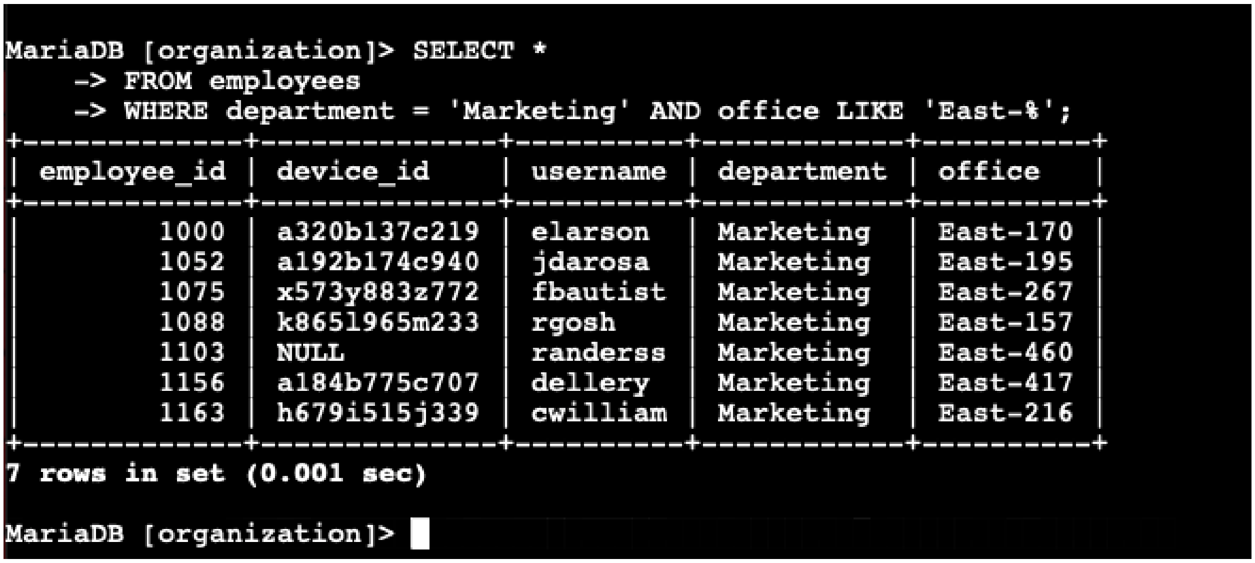
```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE login_date = '2022-05-09' OR login_date = '2022-05-08';
+----------+----------+------------+------------+---------+------------
----+---------+
| event_id | username | login_date | login_time | country | ip_address
    | success |
+----------+----------+------------+------------+---------+------------
----+---------+
|        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 |
|       24 | arusso   | 2022-05-09 | 06:49:39   | MEXICO  | 192.168.171.
192 |       1 |
|       25 | sbaelish | 2022-05-09 | 07:04:02   | US      | 192.168.33.1
37  |       1 |
|       26 | apatel   | 2022-05-08 | 17:27:00   | CANADA  | 192.168.123.
105 |       1 |
|       28 | aestrada | 2022-05-09 | 19:28:12   | MEXICO  | 192.168.27.5
7   |       0 |
|       30 | yappiah  | 2022-05-09 | 03:22:22   | MEX     | 192.168.124.
48  |       1 |
|       32 | acook    | 2022-05-09 | 02:52:02   | CANADA  | 192.168.142.
239 |       0 |
|       36 | asundara | 2022-05-08 | 09:00:42   | US      | 192.168.78.1
51  |       1 |
|       38 | sbaelish | 2022-05-09 | 14:40:01   | USA     | 192.168.60.4
2   |       1 |
|       39 | yappiah  | 2022-05-09 | 07:56:40   | MEXICO  | 192.168.57.1
15  |       1 |
|       42 | cgriffin | 2022-05-09 | 23:04:05   | US      | 192.168.4.15
7   |       0 |
|       43 | mcouliba | 2022-05-08 | 02:35:34   | CANADA  | 192.168.16.2
08  |       0 |
|       44 | daquino  | 2022-05-08 | 07:02:35   | CANADA  | 192.168.168.
144 |       0 |
|       47 | dkot     | 2022-05-08 | 05:06:45   | US      | 192.168.233.
24  |       1 |
|       49 | asundara | 2022-05-08 | 14:00:01   | US      | 192.168.173.
213 |       0 |
|       53 | nmason   | 2022-05-08 | 11:51:38   | CAN     | 192.168.133.
```

Retrieve login attempts outside of Mexico



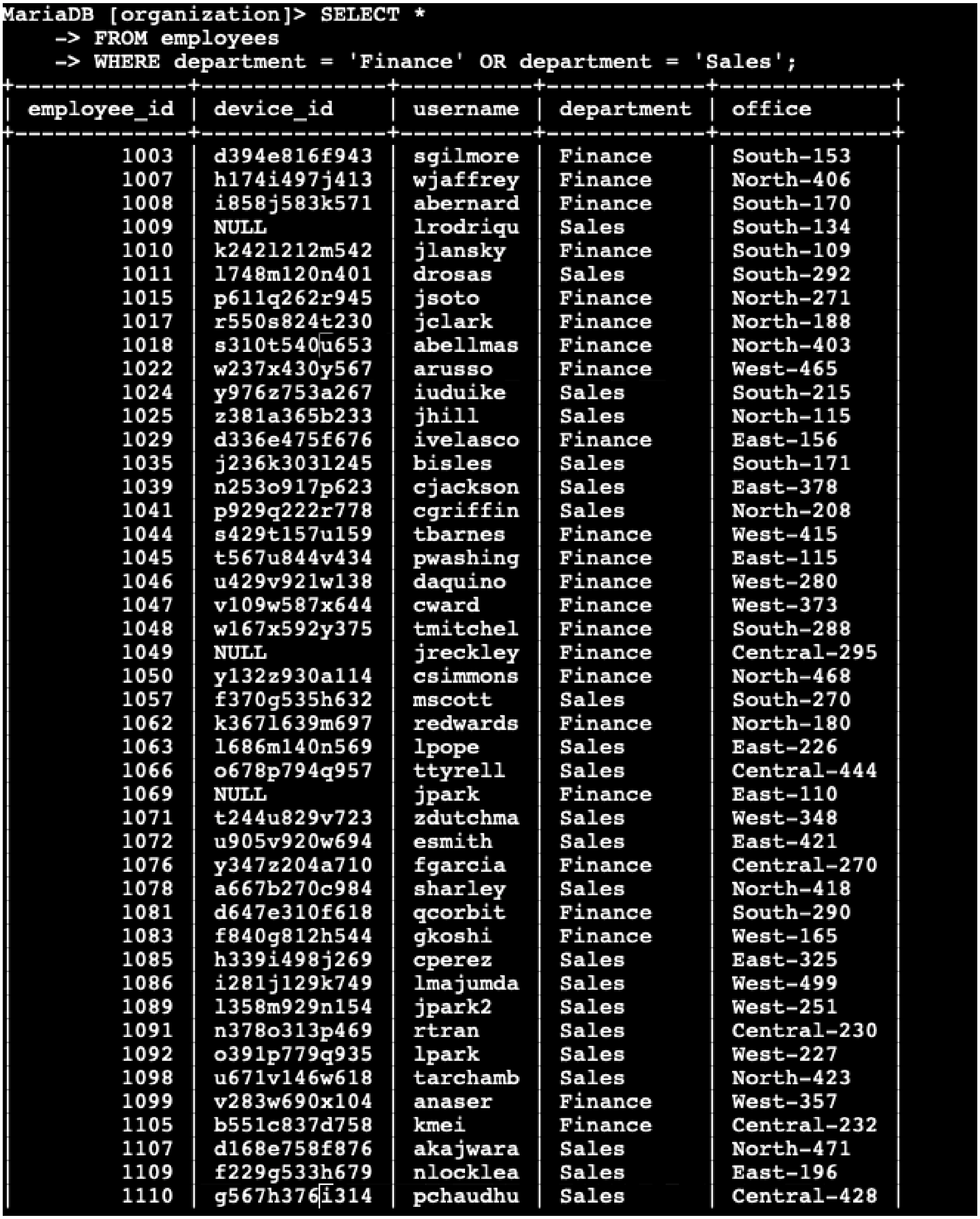
```
MariaDB [organization]> SELECT *
    -> FROM log_in_attempts
    -> WHERE NOT country LIKE 'MEX%';
+----------+----------+------------+------------+---------+------------
----+---------+
| event_id | username | login_date | login_time | country | ip_address
    | success |
+----------+----------+------------+------------+---------+------------
----+---------+
|        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  | 192.168.86.2
32  |       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  | 192.168.140.
81  |       0 |
|       12 | dkot     | 2022-05-08 | 09:11:34   | USA     | 192.168.100.
158 |       1 |
|       13 | mrah     | 2022-05-11 | 09:29:34   | USA     | 192.168.246.
135 |       1 |
|       14 | sbaelish | 2022-05-10 | 10:20:18   | US      | 192.168.16.9
9   |       1 |
|       15 | lyamamot | 2022-05-09 | 17:17:26   | USA     | 192.168.183.
51  |       0 |
|       16 | mcouliba | 2022-05-11 | 06:44:22   | CAN     | 192.168.172.
189 |       1 |
|       17 | pwashing | 2022-05-11 | 02:33:02   | USA     | 192.168.81.8
9   |       1 |
|       18 | pwashing | 2022-05-11 | 19:28:50   | US      | 192.168.66.1
42  |       0 |
|       19 | jhill    | 2022-05-12 | 13:09:04   | US      | 192.168.142.
245 |       1 |
|       21 | iuduike  | 2022-05-11 | 17:50:00   | US      | 192.168.131.
147 |       1 |
|       25 | sbaelish | 2022-05-09 | 07:04:02   | US      | 192.168.33.1
37  |       1 |
|       26 | apatel   | 2022-05-08 | 17:27:00   | CANADA  | 192.168.123.
105 |       1 |
|       29 | bisles   | 2022-05-11 | 01:21:22   | US      | 192.168.85.1
86  |       0 |
```

Retrieve employees in Marketing



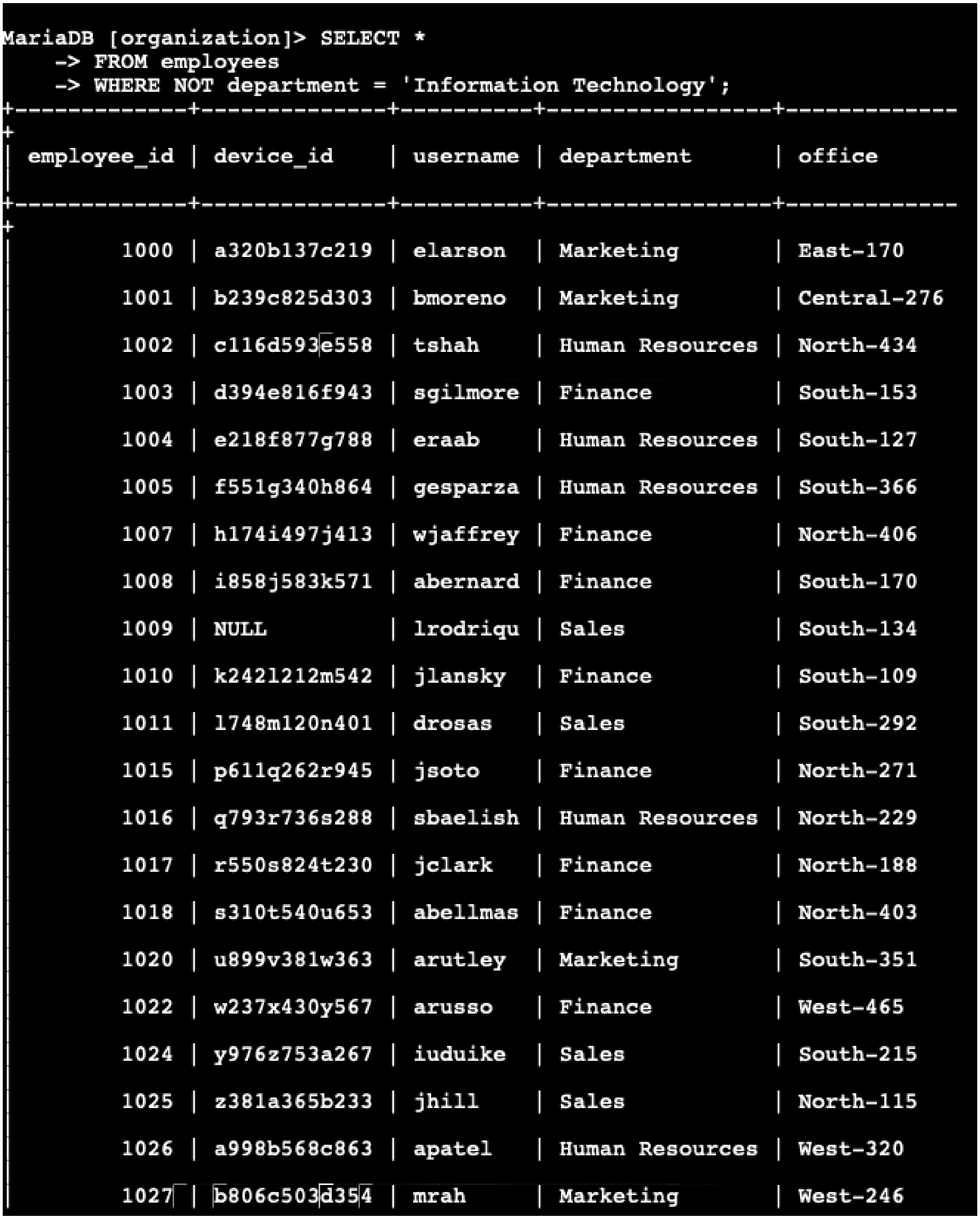
```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Marketing' AND office LIKE 'East-%';
+-------------+--------------+----------+------------+----------+
| employee_id | device_id    | username | department | office   |
+-------------+--------------+----------+------------+----------+
|        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)

MariaDB [organization]> 
```

Retrieve employees in Finance or Sales



```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE department = 'Finance' OR department = '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   |
|        1009 | NULL         | lrodriqu | Sales      | South-134   |
|        1010 | k2421212m542 | jlansky  | Finance    | South-109   |
|        1011 | 1748m120n401 | drosas   | Sales      | South-292   |
|        1015 | p611q262r945 | jsoto    | Finance    | North-271   |
|        1017 | r550s824t230 | jclark   | Finance    | North-188   |
|        1018 | s310t540u653 | abellmas | Finance    | North-403   |
|        1022 | w237x430y567 | arusso   | Finance    | West-465    |
|        1024 | y976z753a267 | iuduike  | Sales      | South-215   |
|        1025 | z381a365b233 | jhill    | Sales      | North-115   |
|        1029 | d336e475f676 | ivelasco | Finance    | East-156    |
|        1035 | j236k3031245 | bisles   | Sales      | South-171   |
|        1039 | n253o917p623 | cjackson | Sales      | East-378    |
|        1041 | p929q222r778 | cgriffin | Sales      | North-208   |
|        1044 | s429t157u159 | tbarnes  | Finance    | West-415    |
|        1045 | t567u844v434 | pwashing | Finance    | East-115    |
|        1046 | u429v921w138 | daquino  | Finance    | West-280    |
|        1047 | v109w587x644 | cward    | Finance    | West-373    |
|        1048 | w167x592y375 | tmitchel | Finance    | South-288   |
|        1049 | NULL         | jreckley | Finance    | Central-295 |
|        1050 | y132z930a114 | csimmons | Finance    | North-468   |
|        1057 | f370g535h632 | mscott   | Sales      | South-270   |
|        1062 | k3671639m697 | redwards | Finance    | North-180   |
|        1063 | 1686m140n569 | lpope    | Sales      | East-226    |
|        1066 | o678p794q957 | ttyrell  | Sales      | Central-444 |
|        1069 | NULL         | jpark    | Finance    | East-110    |
|        1071 | t244u829v723 | zdutchma | Sales      | West-348    |
|        1072 | u905v920w694 | esmith   | Sales      | East-421    |
|        1076 | y347z204a710 | fgarcia  | Finance    | Central-270 |
|        1078 | a667b270c984 | sharley  | Sales      | North-418   |
|        1081 | d647e310f618 | qcorbit  | Finance    | South-290   |
|        1083 | f840g812h544 | gkoshi   | Finance    | West-165    |
|        1085 | h339i498j269 | cperez   | Sales      | East-325    |
|        1086 | i281j129k749 | lmajumda | Sales      | West-499    |
|        1089 | 1358m929n154 | jpark2   | Sales      | West-251    |
|        1091 | n378o313p469 | rtran    | Sales      | Central-230 |
|        1092 | o391p779q935 | lpark    | Sales      | West-227    |
|        1098 | u671v146w618 | tarchamb | Sales      | North-423   |
|        1099 | v283w690x104 | anaser   | Finance    | West-357    |
|        1105 | b551c837d758 | kmei     | Finance    | Central-232 |
|        1107 | d168e758f876 | akajwara | Sales      | North-471   |
|        1109 | f229g533h679 | nlocklea | Sales      | East-196    |
|        1110 | g567h376i314 | pchaudhu | Sales      | Central-428 |
```

Retrieve all employees not in IT



```
MariaDB [organization]> SELECT *
    -> FROM employees
    -> WHERE NOT department = 'Information Technology';
+-------------+--------------+----------+-----------------+-------------
+
| employee_id | device_id    | username | department      | office
|
+-------------+--------------+----------+-----------------+-------------
+
|        1000 | a320b137c219 | elarson  | Marketing       | East-170
|
|        1001 | b239c825d303 | bmoreno  | Marketing       | Central-276
|
|        1002 | c116d593e558 | tshah    | Human Resources | North-434
|
|        1003 | d394e816f943 | sgilmore | Finance         | South-153
|
|        1004 | e218f877g788 | eraab    | Human Resources | South-127
|
|        1005 | f551g340h864 | gesparza | Human Resources | South-366
|
|        1007 | h174i497j413 | wjaffrey | Finance         | North-406
|
|        1008 | i858j583k571 | abernard | Finance         | South-170
|
|        1009 | NULL         | lrodriqu | Sales           | South-134
|
|        1010 | k2421212m542 | jlansky  | Finance         | South-109
|
|        1011 | 1748m120n401 | drosas   | Sales           | South-292
|
|        1015 | p611q262r945 | jsoto    | Finance         | North-271
|
|        1016 | q793r736s288 | sbaelish | Human Resources | North-229
|
|        1017 | r550s824t230 | jclark   | Finance         | North-188
|
|        1018 | s310t540u653 | abellmas | Finance         | North-403
|
|        1020 | u899v381w363 | arutley  | Marketing       | South-351
|
|        1022 | w237x430y567 | arusso   | Finance         | West-465
|
|        1024 | y976z753a267 | iuduike  | Sales           | South-215
|
|        1025 | z381a365b233 | jhill    | Sales           | North-115
|
|        1026 | a998b568c863 | apatel   | Human Resources | West-320
|
|        1027 | b806c503d354 | mrah     | Marketing       | West-246
```

Summary

In the document, I learned how to use SQL commands for filtering database records. I practiced retrieving data based on specific conditions, like time and department. For instance, I used commands to select login attempts outside of usual business hours and to filter out logins from certain geographic locations. I also learned to identify records from particular departments, like employees not in the IT department. Through this, I gained a better understanding of using SQL operators such as `WHERE`, `AND`, `OR`, `NOT`, and `LIKE` for diverse data filtering scenarios.