Name: Isha Dhabalia

Div: A

Roll no.: 1911018

Scenario: There have been discrepancies in the database containing data about the students due to which a database forensic investigator has been called to check the database and investigate.

To create this scenario for forensic investigation the following experiments were carried out:

Step 1: Create Student database

```
/*creating database*/
create database Student;
/*using database*/
use Student;
/*creating tables*/
create table marks(roll_no char(7) PRIMARY KEY,
                    first_name varchar(100) NOT NULL,
                                                last_name varchar(100) NOT NULL,
                    course_number varchar(10),
                    total_marks Int, status char(4));

create table student_details(student_roll char(7) unique,
                     aadhaar_no varchar(12) unique,
                     student_first_name varchar(100) NOT NULL,
                     student_last_name varchar(100) NOT NULL,
                     contact_number Int,
                     foreign key(student_roll) references marks(roll_no));
/*altering tables*/

ALTER TABLE marks
```

```
RENAME COLUMN status TO result_status;

alter table student_details
modify column contact_number Long;

/*inserting values into table*/
insert into marks(roll_no,first_name,last_name,course_number,total_marks)
values("2111001","Ekansh","Sharma","RD2021001",60);
insert into marks(roll_no,first_name,last_name,course_number,total_marks)
values("2111002","Shivangi","Lal","RD2021001",75),
    ("2111003","Ekta","Rathore","RD2021001",99),
    ("2111004","Diya","Singh","RD2021001",80),
    ("2111005","Ananya","Bansal","RD2021001",36),
    ("2111006","Rahul","Bose","RD2021001",44),
    ("2111007","Dimple","Seth","RD2021001",54),
    ("2111008","Harpreet","Kaur","RD2021001",39),
    ("2111009","Harichandra","Iyer","RD2021001",90),
    ("2111010","Raghav","Agrawal","RD2021001",77);

/*updating marks table*/
update marks set result_status=if(total_marks>=40,"PASS","FAIL");

/*inserting values into table*/
insert into
student_details(student_roll,aadhaar_no,student_first_name,student_last_name,contact_numb
er)
values("2111001","444433332222","Ekansh","Sharma",9732421408),
    ("2111002","000011112222","Shivangi","Lal",9635586571),
    ("2111003","123412345555","Ekta","Rathore",9474055775),
    ("2111004","789212349999","Diya","Singh",9232687509),
    ("2111005","987609843213","Ananya","Bansal",8972193052),
```

("2111006","990723431233","Rahul","Bose",9732157880),

("2111007","876556562234","Dimple","Seth",9732119608),

("2111008","454477778876","Harpreet","Kaur",9609514553),

("2111009","323311355678","Harichandra","Iyer",8145622754),

("2111010","989877675422","Raghav","Agrawal",9002622754);

Before corrupting database:

marks table

```
mysql> use Student
Database changed
mysql> select * from marks;
+---------+------------+-----------+---------------+------------+---------------+
| roll_no | first_name | last_name | course_number | total_marks | result_status |
+---------+------------+-----------+---------------+------------+---------------+
| 2111001 | Ekansh     | Sharma    | RD2021001     |          60 | PASS          |
| 2111002 | Shivangi   | Lal       | RD2021001     |          75 | PASS          |
| 2111003 | Ekta       | Rathore   | RD2021001     |          99 | PASS          |
| 2111004 | Diya       | Singh     | RD2021001     |          80 | PASS          |
| 2111005 | Ananya     | Bansal    | RD2021001     |          36 | FAIL          |
| 2111006 | Rahul      | Bose      | RD2021001     |          44 | PASS          |
| 2111007 | Dimple     | Seth      | RD2021001     |          54 | PASS          |
| 2111008 | Harpreet   | Kaur      | RD2021001     |          39 | FAIL          |
| 2111009 | Harichandra | Iyer     | RD2021001     |          90 | PASS          |
| 2111010 | Raghav     | Agrawal   | RD2021001     |          77 | PASS          |
+---------+------------+-----------+---------------+------------+---------------+
10 rows in set (0.00 sec)
```

student_details table

```
mysql> select * from student_details;
+--------------+--------------+--------------------+-------------------+----------------+
| student_roll | aadhaar_no   | student_first_name | student_last_name | contact_number |
+--------------+--------------+--------------------+-------------------+----------------+
| 2111001      | 444433332222 | Ekansh             | Sharma            | 9732421408     |
| 2111002      | 000011112222 | Shivangi           | Lal               | 9635586571     |
| 2111003      | 123412345555 | Ekta               | Rathore           | 9474055775     |
| 2111004      | 789212349999 | Diya               | Singh             | 9232687509     |
| 2111005      | 987609843213 | Ananya             | Bansal            | 8972193052     |
| 2111006      | 990723431233 | Rahul              | Bose              | 9732157880     |
| 2111007      | 876556562234 | Dimple             | Seth              | 9732119608     |
| 2111008      | 454477778876 | Harpreet           | Kaur              | 9609514553     |
| 2111009      | 323311355678 | Harichandra        | Iyer              | 8145622754     |
| 2111010      | 989877675422 | Raghav             | Agrawal           | 9002622754     |
+--------------+--------------+--------------------+-------------------+----------------+
10 rows in set (0.00 sec)
```

STEP 2: MAKING A COPY OF STUDENT DATABASE FOR BACKUP

Create a database Student1 for backup

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| hrapp              |
| information_schema |
| mysql              |
| nationalparkdb     |
| nationalparksystem |
| performance_schema |
| sakila             |
| student            |
| sys                |
| world              |
+--------------------+
10 rows in set (0.01 sec)

mysql> create database Student1;
Query OK, 1 row affected (0.01 sec)

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| hrapp              |
| information_schema |
| mysql              |
| nationalparkdb     |
| nationalparksystem |
| performance_schema |
| sakila             |
| student            |
| student1           |
| sys                |
| world              |
+--------------------+
11 rows in set (0.00 sec)
```

Currently there are no tables in database Student1 as the database has not been copied

```
mysql> use Student1;
Database changed
mysql> show tables;
Empty set (0.00 sec)
```

Using mysqldump copy the database Student into a sql file and then copy that file into Student1 database

```
C:\Users\Isha>cd C:\Program Files\MySQL\MySQL Server 8.0\bin

C:\Program Files\MySQL\MySQL Server 8.0\bin>mysqldump -u root -p Student > D:\Database_backup\Studentdb.sql
Enter password: **********

C:\Program Files\MySQL\MySQL Server 8.0\bin>mysql -u root -p Student1 < D:\Database_backup\Studentdb.sql
Enter password: **********
```

The Student1 database is now a copy of the Student database

```
C:\Program Files\MySQL\MySQL Server 8.0\bin>mysql -uroot -p
Enter password: **********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 30
Server version: 8.0.23 MySQL Community Server - GPL

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use Student1;
Database changed
mysql> show tables;
+--------------------+
| Tables_in_student1 |
+--------------------+
| marks              |
| student_details    |
+--------------------+
2 rows in set (0.01 sec)

mysql> use Student;
Database changed
mysql> show tables;
+-------------------+
| Tables_in_student |
+-------------------+
| marks             |
| student_details   |
+-------------------+
2 rows in set (0.00 sec)
```

Create a scenario for forensic investigation by corrupting the layers of database

STEP 3: SIMULATED EXPERIMENT ON APPLICATION DATA LAYER

The Application data layer is modified by creating a column in the table marks of Student database

```
mysql> ALTER table marks ADD
    -> temp varchar (20)
    -> AFTER last_name;
```

```
mysql> select * from marks;
+---------+------------+-----------+------+---------------+-------------+---------------+
| roll_no | first_name | last_name | temp | course_number | total_marks | result_status |
+---------+------------+-----------+------+---------------+-------------+---------------+
| 2111001 | Ekansh     | Sharma    | NULL | RD2021001     |          60 | PASS          |
| 2111002 | Shivangi   | Lal       | NULL | RD2021001     |          75 | PASS          |
| 2111003 | Ekta       | Rathore   | NULL | RD2021001     |          99 | PASS          |
| 2111004 | Diya       | Singh     | NULL | RD2021001     |          80 | PASS          |
| 2111005 | Ananya     | Bansal    | NULL | RD2021001     |          36 | FAIL          |
| 2111006 | Rahul      | Bose      | NULL | RD2021001     |          44 | PASS          |
| 2111007 | Dimple     | Seth      | NULL | RD2021001     |          54 | PASS          |
| 2111008 | Harpreet   | Kaur      | NULL | RD2021001     |          39 | FAIL          |
| 2111009 | Harichandra| Iyer      | NULL | RD2021001     |          90 | PASS          |
| 2111010 | Raghav     | Agrawal   | NULL | RD2021001     |          77 | PASS          |
+---------+------------+-----------+------+---------------+-------------+---------------+
10 rows in set (0.00 sec)
```

The data from column last_name is copied into column temp

```
mysql> UPDATE marks SET temp=last_name;
Query OK, 10 rows affected (0.01 sec)
Rows matched: 10  Changed: 10  Warnings: 0

mysql> select * from marks;
+---------+------------+-----------+---------+---------------+-------------+---------------+
| roll_no | first_name | last_name | temp    | course_number | total_marks | result_status |
+---------+------------+-----------+---------+---------------+-------------+---------------+
| 2111001 | Ekansh     | Sharma    | Sharma  | RD2021001     |          60 | PASS          |
| 2111002 | Shivangi   | Lal       | Lal     | RD2021001     |          75 | PASS          |
| 2111003 | Ekta       | Rathore   | Rathore | RD2021001     |          99 | PASS          |
| 2111004 | Diya       | Singh     | Singh   | RD2021001     |          80 | PASS          |
| 2111005 | Ananya     | Bansal    | Bansal  | RD2021001     |          36 | FAIL          |
| 2111006 | Rahul      | Bose      | Bose    | RD2021001     |          44 | PASS          |
| 2111007 | Dimple     | Seth      | Seth    | RD2021001     |          54 | PASS          |
| 2111008 | Harpreet   | Kaur      | Kaur    | RD2021001     |          39 | FAIL          |
| 2111009 | Harichandra| Iyer      | Iyer    | RD2021001     |          90 | PASS          |
| 2111010 | Raghav     | Agrawal   | Agrawal | RD2021001     |          77 | PASS          |
+---------+------------+-----------+---------+---------------+-------------+---------------+
10 rows in set (0.00 sec)
```

The data from column first_name is copied into column temp by command

UPDATE marks set last_name=first_name

```
mysql> select * from marks;
+---------+-------------+-------------+---------+---------------+-------------+---------------+
| roll_no | first_name  | last_name   | temp    | course_number | total_marks | result_status |
+---------+-------------+-------------+---------+---------------+-------------+---------------+
| 2111001 | Ekansh      | Ekansh      | Sharma  | RD2021001     |          60 | PASS          |
| 2111002 | Shivangi    | Shivangi    | Lal     | RD2021001     |          75 | PASS          |
| 2111003 | Ekta        | Ekta        | Rathore | RD2021001     |          99 | PASS          |
| 2111004 | Diya        | Diya        | Singh   | RD2021001     |          80 | PASS          |
| 2111005 | Ananya      | Ananya      | Bansal  | RD2021001     |          36 | FAIL          |
| 2111006 | Rahul       | Rahul       | Bose    | RD2021001     |          44 | PASS          |
| 2111007 | Dimple      | Dimple      | Seth    | RD2021001     |          54 | PASS          |
| 2111008 | Harpreet    | Harpreet    | Kaur    | RD2021001     |          39 | FAIL          |
| 2111009 | Harichandra | Harichandra | Iyer    | RD2021001     |          90 | PASS          |
| 2111010 | Raghav      | Raghav      | Agrawal | RD2021001     |          77 | PASS          |
+---------+-------------+-------------+---------+---------------+-------------+---------------+
10 rows in set (0.00 sec)
```

The data from column temp is copied into column first_name

```
mysql> UPDATE marks SET first_name=temp;
Query OK, 10 rows affected (0.01 sec)
Rows matched: 10  Changed: 10  Warnings: 0

mysql> select * from marks;
+---------+------------+-------------+---------+---------------+-------------+---------------+
| roll_no | first_name | last_name   | temp    | course_number | total_marks | result_status |
+---------+------------+-------------+---------+---------------+-------------+---------------+
| 2111001 | Sharma     | Ekansh      | Sharma  | RD2021001     |          60 | PASS          |
| 2111002 | Lal        | Shivangi    | Lal     | RD2021001     |          75 | PASS          |
| 2111003 | Rathore    | Ekta        | Rathore | RD2021001     |          99 | PASS          |
| 2111004 | Singh      | Diya        | Singh   | RD2021001     |          80 | PASS          |
| 2111005 | Bansal     | Ananya      | Bansal  | RD2021001     |          36 | FAIL          |
| 2111006 | Bose       | Rahul       | Bose    | RD2021001     |          44 | PASS          |
| 2111007 | Seth       | Dimple      | Seth    | RD2021001     |          54 | PASS          |
| 2111008 | Kaur       | Harpreet    | Kaur    | RD2021001     |          39 | FAIL          |
| 2111009 | Iyer       | Harichandra | Iyer    | RD2021001     |          90 | PASS          |
| 2111010 | Agrawal    | Raghav      | Agrawal | RD2021001     |          77 | PASS          |
+---------+------------+-------------+---------+---------------+-------------+---------------+
10 rows in set (0.00 sec)
```

The column temp is dropped from marks table

```
mysql> ALTER TABLE marks DROP COLUMN temp;
Query OK, 0 rows affected (0.13 sec)
Records: 0  Duplicates: 0  Warnings: 0

mysql> select * from marks;
+---------+------------+-------------+---------------+-------------+---------------+
| roll_no | first_name | last_name   | course_number | total_marks | result_status |
+---------+------------+-------------+---------------+-------------+---------------+
| 2111001 | Sharma     | Ekansh      | RD2021001     |          60 | PASS          |
| 2111002 | Lal        | Shivangi    | RD2021001     |          75 | PASS          |
| 2111003 | Rathore    | Ekta        | RD2021001     |          99 | PASS          |
| 2111004 | Singh      | Diya        | RD2021001     |          80 | PASS          |
| 2111005 | Bansal     | Ananya      | RD2021001     |          36 | FAIL          |
| 2111006 | Bose       | Rahul       | RD2021001     |          44 | PASS          |
| 2111007 | Seth       | Dimple      | RD2021001     |          54 | PASS          |
| 2111008 | Kaur       | Harpreet    | RD2021001     |          39 | FAIL          |
| 2111009 | Iyer       | Harichandra | RD2021001     |          90 | PASS          |
| 2111010 | Agrawal    | Raghav      | RD2021001     |          77 | PASS          |
+---------+------------+-------------+---------------+-------------+---------------+
10 rows in set (0.00 sec)
```

When the columns roll_number, first_name,last_name from marks table and the columns student_roll, student_first_name and student_last_name from student_details table are viewed there are discrepancies in the data.

```
mysql> use Student;
Database changed
mysql> select roll_no,first_name,last_name from marks;
+---------+------------+-------------+
| roll_no | first_name | last_name   |
+---------+------------+-------------+
| 2111001 | Sharma     | Ekansh      |
| 2111002 | Lal        | Shivangi    |
| 2111003 | Rathore    | Ekta        |
| 2111004 | Singh      | Diya        |
| 2111005 | Bansal     | Ananya      |
| 2111006 | Bose       | Rahul       |
| 2111007 | Seth       | Dimple      |
| 2111008 | Kaur       | Harpreet    |
| 2111009 | Iyer       | Harichandra |
| 2111010 | Agrawal    | Raghav      |
+---------+------------+-------------+
10 rows in set (0.00 sec)
```

```
mysql> select student_roll,student_first_name,student_last_name from student_details;
+--------------+--------------------+-------------------+
| student_roll | student_first_name | student_last_name |
+--------------+--------------------+-------------------+
| 2111001      | Ekansh             | Sharma            |
| 2111002      | Shivangi           | Lal               |
| 2111003      | Ekta               | Rathore           |
| 2111004      | Diya               | Singh             |
| 2111005      | Ananya             | Bansal            |
| 2111006      | Rahul              | Bose              |
| 2111007      | Dimple             | Seth              |
| 2111008      | Harpreet           | Kaur              |
| 2111009      | Harichandra        | Iyer              |
| 2111010      | Raghav             | Agrawal           |
+--------------+--------------------+-------------------+
10 rows in set (0.00 sec)
```

When the backup database Student1 is viewed the data from tables marks and student_details match

```
mysql> use Student1;
Database changed
mysql> select roll_no,first_name,last_name from marks;
+---------+------------+-----------+
| roll_no | first_name | last_name |
+---------+------------+-----------+
| 2111001 | Ekansh     | Sharma    |
| 2111002 | Shivangi   | Lal       |
| 2111003 | Ekta       | Rathore   |
| 2111004 | Diya       | Singh     |
| 2111005 | Ananya     | Bansal    |
| 2111006 | Rahul      | Bose      |
| 2111007 | Dimple     | Seth      |
| 2111008 | Harpreet   | Kaur      |
| 2111009 | Harichandra | Iyer     |
| 2111010 | Raghav     | Agrawal   |
+---------+------------+-----------+
10 rows in set (0.00 sec)

mysql> select student_roll,student_first_name,student_last_name from student_details;
+--------------+--------------------+-------------------+
| student_roll | student_first_name | student_last_name |
+--------------+--------------------+-------------------+
| 2111001      | Ekansh             | Sharma            |
| 2111002      | Shivangi           | Lal               |
| 2111003      | Ekta               | Rathore           |
| 2111004      | Diya               | Singh             |
| 2111005      | Ananya             | Bansal            |
| 2111006      | Rahul              | Bose              |
| 2111007      | Dimple             | Seth              |
| 2111008      | Harpreet           | Kaur              |
| 2111009      | Harichandra        | Iyer              |
| 2111010      | Raghav             | Agrawal           |
+--------------+--------------------+-------------------+
10 rows in set (0.00 sec)
```

The total_marks column was modified

```
mysql> update marks
    -> set total_marks=56
    -> where roll_no="2111005";
Query OK, 1 row affected (0.01 sec)
Rows matched: 1  Changed: 1  Warnings: 0

mysql> update marks
    -> set total_marks=88
    -> where roll_no="2111008";
Query OK, 1 row affected (0.01 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

The result_status column was modified

```
mysql> update marks set result_status=if(total_marks>=40,"PASS","FAIL");
Query OK, 2 rows affected (0.05 sec)
Rows matched: 10  Changed: 2  Warnings: 0

mysql> select * from marks;
+---------+------------+-------------+---------------+-------------+---------------+
| roll_no | first_name | last_name   | course_number | total_marks | result_status |
+---------+------------+-------------+---------------+-------------+---------------+
| 2111001 | Sharma     | Ekansh      | RD2021001     |          60 | PASS          |
| 2111002 | Lal        | Shivangi    | RD2021001     |          75 | PASS          |
| 2111003 | Rathore    | Ekta        | RD2021001     |          99 | PASS          |
| 2111004 | Singh      | Diya        | RD2021001     |          80 | PASS          |
| 2111005 | Bansal     | Ananya      | RD2021001     |          56 | PASS          |
| 2111006 | Bose       | Rahul       | RD2021001     |          44 | PASS          |
| 2111007 | Seth       | Dimple      | RD2021001     |          54 | PASS          |
| 2111008 | Kaur       | Harpreet    | RD2021001     |          88 | PASS          |
| 2111009 | Iyer       | Harichandra | RD2021001     |          90 | PASS          |
| 2111010 | Agrawal    | Raghav      | RD2021001     |          77 | PASS          |
+---------+------------+-------------+---------------+-------------+---------------+
10 rows in set (0.00 sec)
```

When the total number of students who have passed is viewed it shows that all students have passed which is suspicious

```
mysql> use Student;
Database changed
mysql> select count(*)
    -> from marks
    -> where result_status="PASS";
+----------+
| count(*) |
+----------+
|       10 |
+----------+
1 row in set (0.01 sec)
```

When the total number of students who have passed is viewed using the backup database Student1, the count is different

```
mysql> use Student1;
Database changed
mysql> select count(*)
    -> from marks
    ->  where result_status="PASS";
+----------+
| count(*) |
+----------+
|        8 |
+----------+
1 row in set (0.00 sec)
```

When both databases are viewed, there are discrepancies in the databases

```
mysql> use Student;
Database changed
mysql> select * from marks;
+---------+------------+-------------+---------------+-------------+---------------+
| roll_no | first_name | last_name   | course_number | total_marks | result_status |
+---------+------------+-------------+---------------+-------------+---------------+
| 2111001 | Sharma     | Ekansh      | RD2021001     |          60 | PASS          |
| 2111002 | Lal        | Shivangi    | RD2021001     |          75 | PASS          |
| 2111003 | Rathore    | Ekta        | RD2021001     |          99 | PASS          |
| 2111004 | Singh      | Diya        | RD2021001     |          80 | PASS          |
| 2111005 | Bansal     | Ananya      | RD2021001     |          56 | PASS          |
| 2111006 | Bose       | Rahul       | RD2021001     |          44 | PASS          |
| 2111007 | Seth       | Dimple      | RD2021001     |          54 | PASS          |
| 2111008 | Kaur       | Harpreet    | RD2021001     |          88 | PASS          |
| 2111009 | Iyer       | Harichandra | RD2021001     |          90 | PASS          |
| 2111010 | Agrawal    | Raghav      | RD2021001     |          77 | PASS          |
+---------+------------+-------------+---------------+-------------+---------------+
10 rows in set (0.00 sec)
```

```
mysql> use Student1;
Database changed
mysql> select * from marks;
+---------+-------------+-----------+---------------+-------------+---------------+
| roll_no | first_name  | last_name | course_number | total_marks | result_status |
+---------+-------------+-----------+---------------+-------------+---------------+
| 2111001 | Ekansh      | Sharma    | RD2021001     |          60 | PASS          |
| 2111002 | Shivangi    | Lal       | RD2021001     |          75 | PASS          |
| 2111003 | Ekta        | Rathore   | RD2021001     |          99 | PASS          |
| 2111004 | Diya        | Singh     | RD2021001     |          80 | PASS          |
| 2111005 | Ananya      | Bansal    | RD2021001     |          36 | FAIL          |
| 2111006 | Rahul       | Bose      | RD2021001     |          44 | PASS          |
| 2111007 | Dimple      | Seth      | RD2021001     |          54 | PASS          |
| 2111008 | Harpreet    | Kaur      | RD2021001     |          39 | FAIL          |
| 2111009 | Harichandra | Iyer      | RD2021001     |          90 | PASS          |
| 2111010 | Raghav      | Agrawal   | RD2021001     |          77 | PASS          |
+---------+-------------+-----------+---------------+-------------+---------------+
10 rows in set (0.00 sec)
```

STEP 4: SIMULATED EXPERIMENT ON DATA MODEL LAYER

mysql directory is deleted using Windows PowerShell which is run as an administrator

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> Remove-item "C:\ProgramData\MySQL\MySQL Server 8.0\Data\mysql"
```

As the mysql directory has been deleted the user is unable to access the database

```
mysql> use Student;
ERROR 1049 (42000): Unknown database 'student'
mysql> use Student1;
ERROR 1049 (42000): Unknown database 'student1'
```

STEP 5: FORENSIC REPORT

- When the marks table and student_details table of Student database are accessed, there are the following discrepancies:
    - The first names and last names of the students don't match in both the tables
    - All the students enrolled in the course have passed which is suspicious
- The Student database is compared with the backup database Student1 and it is found that it does not match
- Thus, it can be concluded that there are changes made to the Application Data layer
- In the further investigation when the databases Student and Student1 cannot be accessed. Due to this fact it can be concluded that there are changes in the Data Model Layer