**STATE/CITY WISE CYBER CRIME**

**MOTIVES**

**TABLE OF CONTENTS**

|  |  |
| --- | --- |
| Tittle | Page no |
| ABSTRACTION | 01 |
| FUNCTIONALITIES | 01-02 |
| MODULES | 02-03 |
| ER-DIAGRAM | 03-04 |
| SCHEMA DIAGRAM | 04-05 |
| TABLES CREATION AND INSERTIONS | 05-17 |

01

ABSTRACT

The case study focuses on designing database that stores information regarding cybercrimes in metropolitan cities. Cybercrime refers to illegal activities conducted in cyber space, targeting computer systems, networks and individuals for financial gain or disruption. These activities include ransomware attacks, identity theft hacking etc. Cybercrimes are considered a major risk because they have devastating effects like financial loses, breaches of sensitive data and also it can affect the victim’s reputation and life.

Cybercrime is a growing problem in metropolitan cities/states. This case study examines the motives of cyber criminals in the cities/states. The study found that the most common motives for cybercrimes are revenge, sexual exploitation, political reasons and toxic ideologies. Cyber criminals are increasingly using complex techniques to steal data commit fraud and disrupt operations. The schema in the DBMS includes relations which accommodate information about cities/states, victims, cybercriminals, statistics of the crime rate and the motives behind them etc. The functionalities of this software allow user to retrieve, store, update, insert and delete data in a secured manner.

To conclude, the utilization of a DBMS for this case study enables efficient data management and the exploration, facilitating a deeper understanding of the motives behind cybercriminal activities in a specified metropolitan context. The result of this study can aid law enforcement agencies, policy makers and cyber security professionals in devising targeted strategies to mitigate cyber threads and enhance the digital resilience of urban environment.

FUNCTIONALITIES:

1. User Registration and Authentication:

i) Allow users to create accounts and log in securely.

ii)Implement role-based access control(P,O), with appropriate permissions

2. Data collection and storage:

i) The database accumulates and stores various types of cybercrime data, including Incident reports, attacks patterns, malware signatures, and other relevant information.

3. Search and Retrieval:

i) Provide a search feature to find statistics, details of the case based on various c keywords.

ii) Implement advanced search options such as filtering by year or city.

4. User Profiles:

02

i) Enable users to update their profiles and change passwords.

5. Victim information:

i) Maintains details about affected victims or organizations, their vulnerabilities and the impact of cyber incidents on them.

6. Malware analysis and signature:

i) Includes information on different malware strains, their behaviour, characteristics, and known signatures to aid in identification and defense.

7. Backup and Restore:

i) Regularly backup the database and provide a restore option in case of data loss.

8. Security:

i) Implement security measures like encryption, SQL injection prevention, and user access control.

MODULES:

1. User Authentication and Authorization module:

i) User registration and login system.

ii) Different user roles (P,O) with varying access levels.

2. Data collection and storage module :

i)Stores data .

ii) Includes incident report ,attack patterns ,malware signatures and other information .

3. Search module :

i) Search options with the help of keywords and filtering options.

4. Victim module :

i) Victim details .

ii)Their impacts on cybercrime .

5. Malware analysis module :

i) Store information of malware strains

ii) Helps in identifying known crime signatures for identification and defense.

6.Backup module :

i) Back up and provide restoration.

7.Security module :

03

i) Provides user control

ii) Ensures the integrity of data.

ENTITY RELATIONSHIP DIAGRAM:

ENTITIES:

1.User

2.Victim

3.Accused

4.City

5.Statistics

6.Case

7.Cybercrime

8.Investigator

CARDINALITY:

1.Many to Many (User to Statistics)

2.One to One (Statistics to City)

3.One to Many (City/State to Case)

4.One to One (Case to Accused)

5.One to Many (Accused to cybercrime)

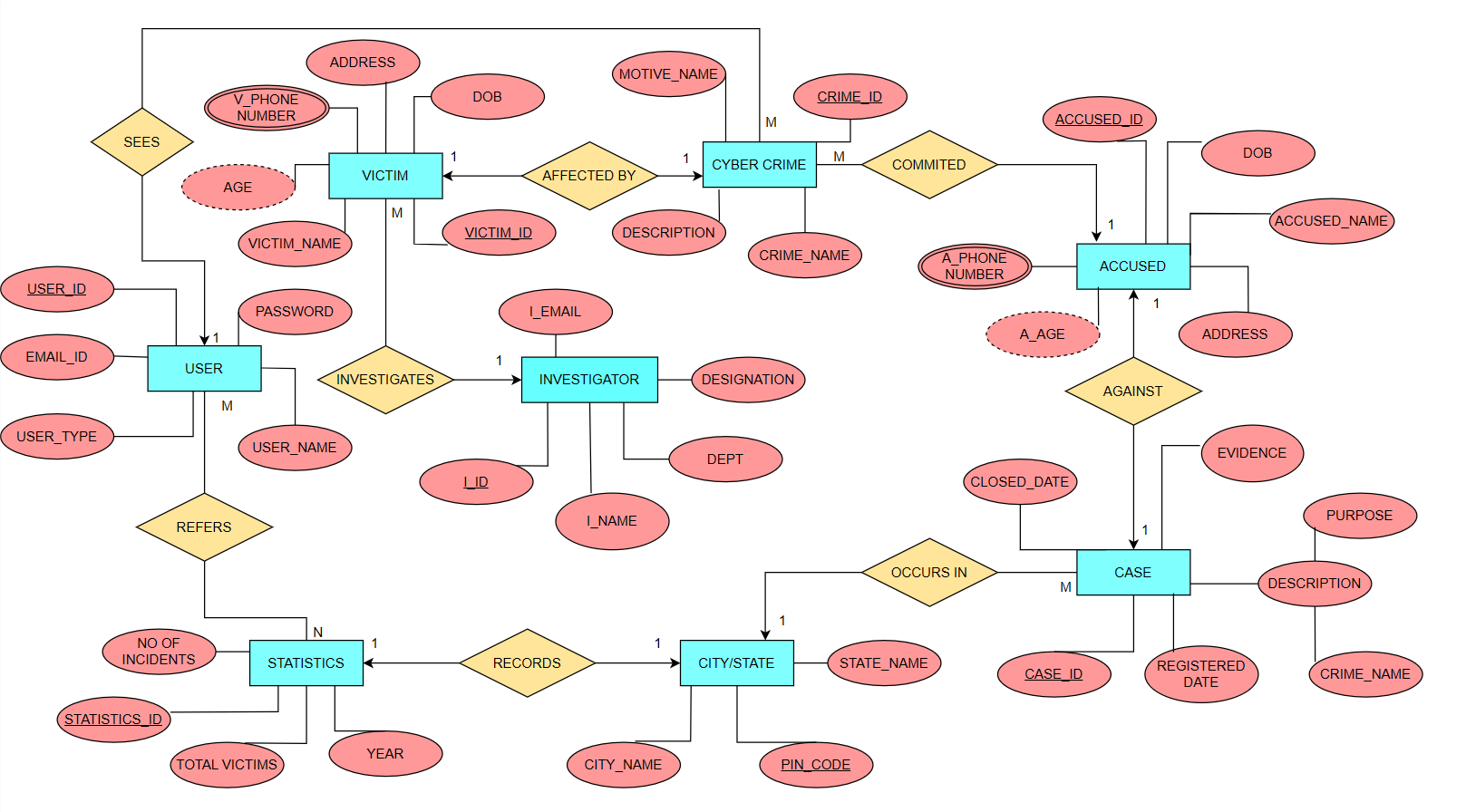
6.One to One (Cybercrime to Victim)

7.Many to One (Victim to Investigator)

8.One to Many (User to Cybercrime)

04

ER DIAGRAM:



ER to Schema:

USER (user\_id, email\_id, user\_type, user\_name, password)

STATISTICS (Statistics\_id,year, no\_of\_incidents, time\_period, total\_victims, pin\_code)

REFERS (user\_id, statistics\_id)

CITY (pin\_code, state\_name, city\_name)

CASE (case\_id, registered\_date, crime\_name, purpose, evidence, closed\_date, pin\_code)

ACCUSED (accused\_id, dob, accused\_name, address, case\_id)

A\_PHONENUMBER (accused\_id, a\_phonenumber)

CYBERCRIME (crime\_id, crime\_name, motive\_name, description, accused\_id, user\_id)

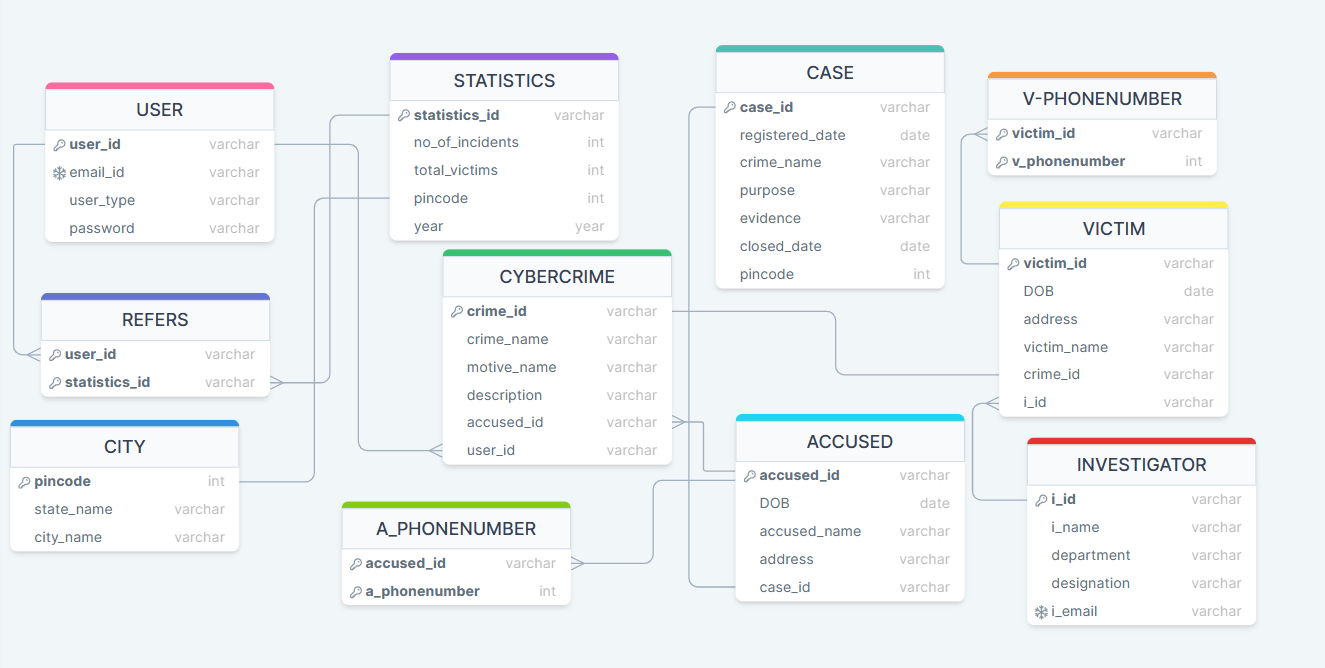
VICTIM (victim\_id, dob, address, victim\_name, crime\_id, i\_id)

V\_PHONENUMBER (victim\_id, v\_phonenumber)

INVESTIGATOR (i\_id, i\_name, dept, designation,i\_email)

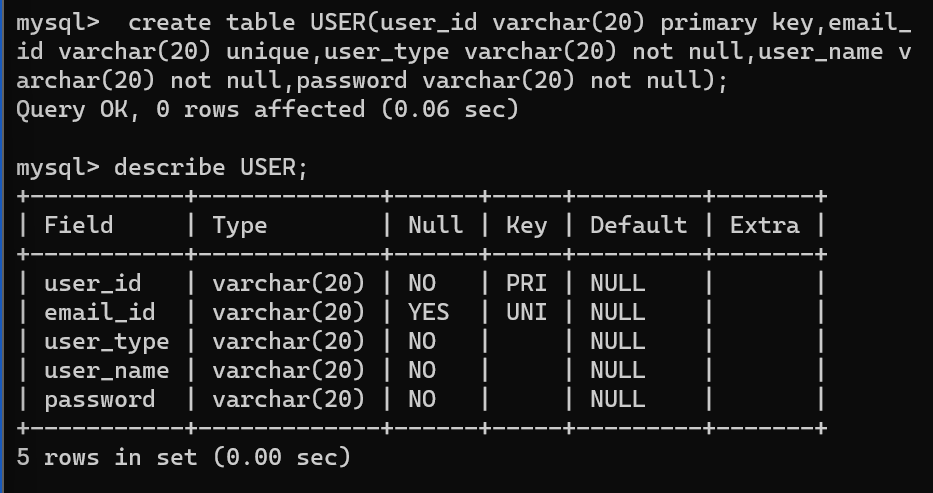
05

Schema Diagram:

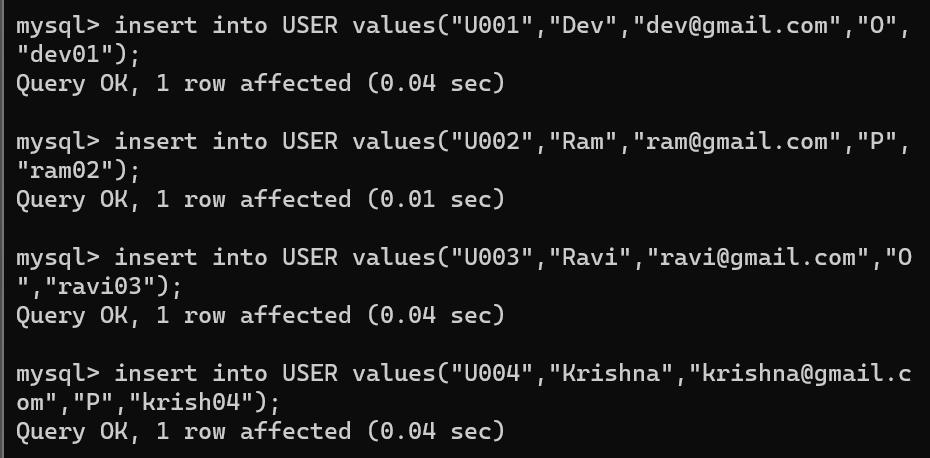


Creation of Tables and Queries:

USER (user\_id, email\_id, user\_type, user\_name, password)



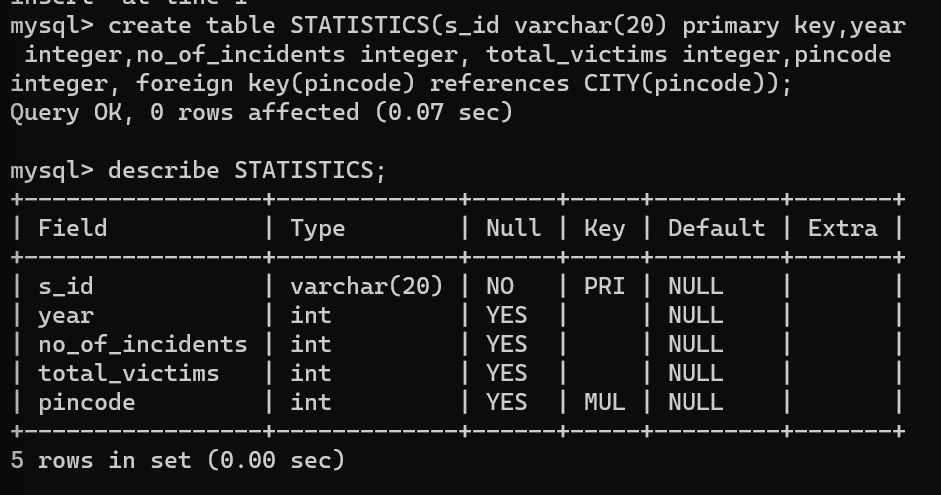
06

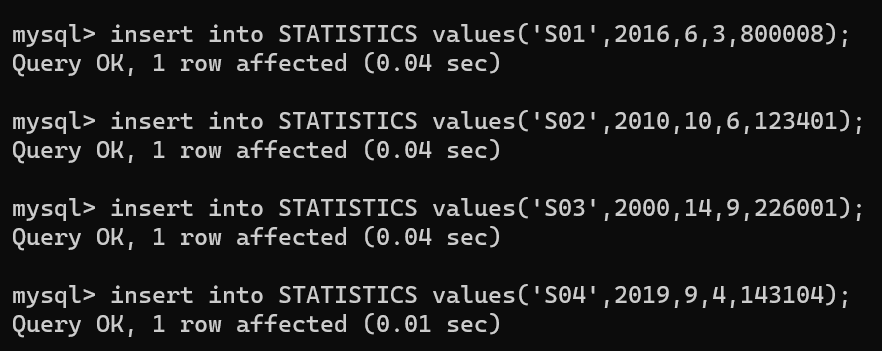


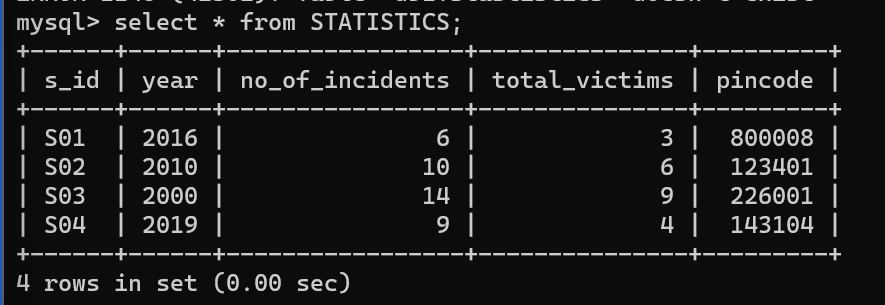


STATISTICS (s\_id,year,no\_of\_incidents, total\_victims, pincode)

07

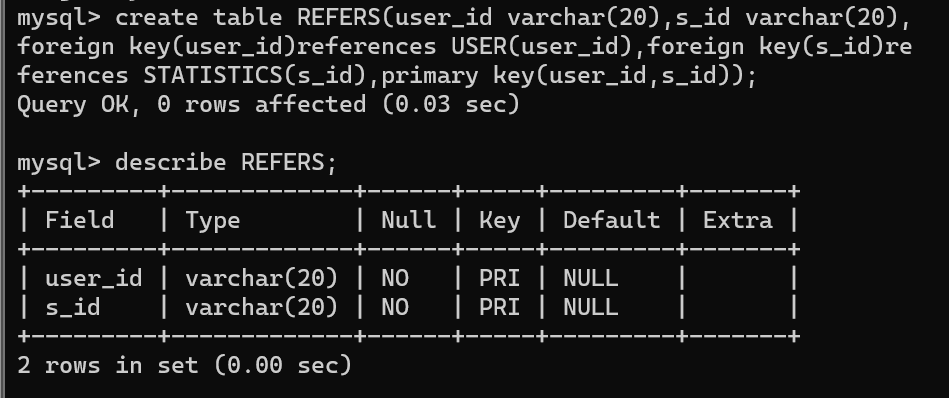


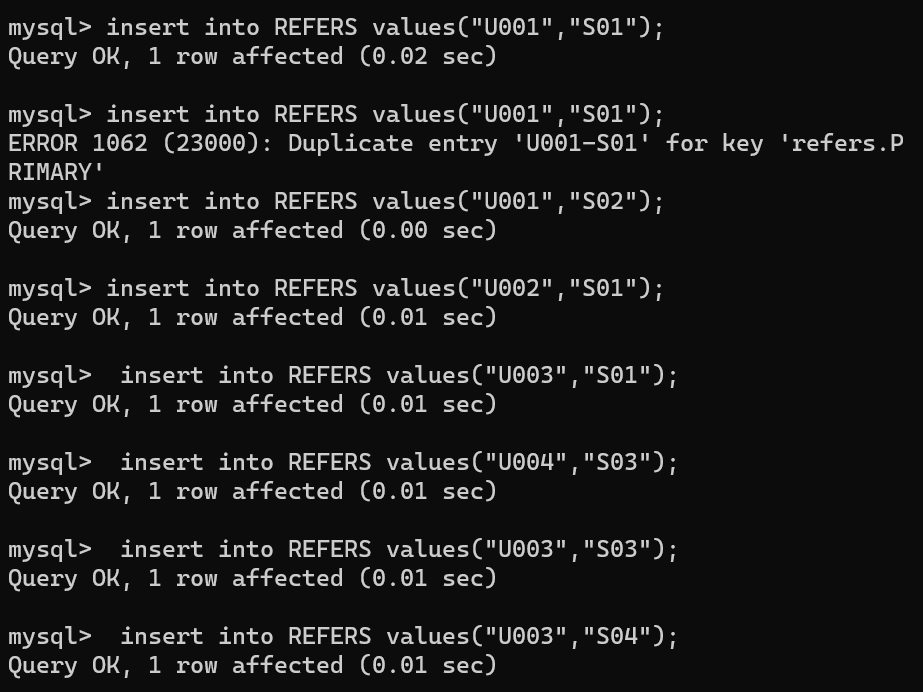




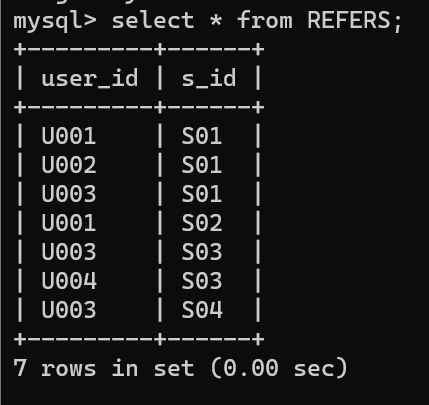
REFERS (user\_id, s\_id)

08

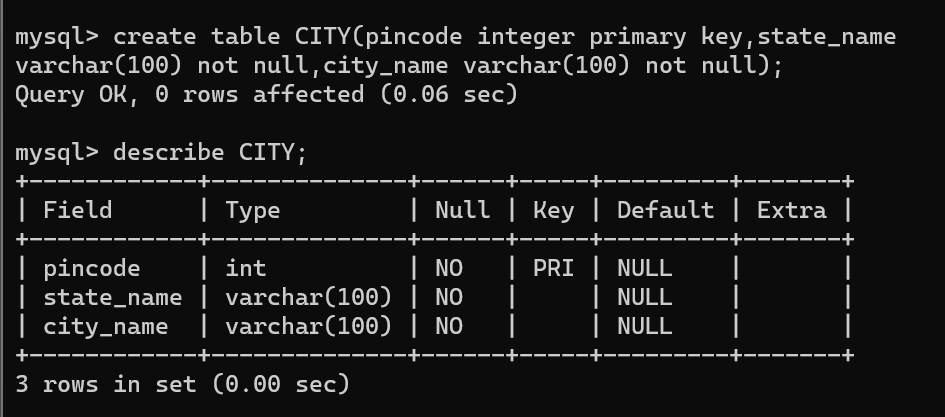




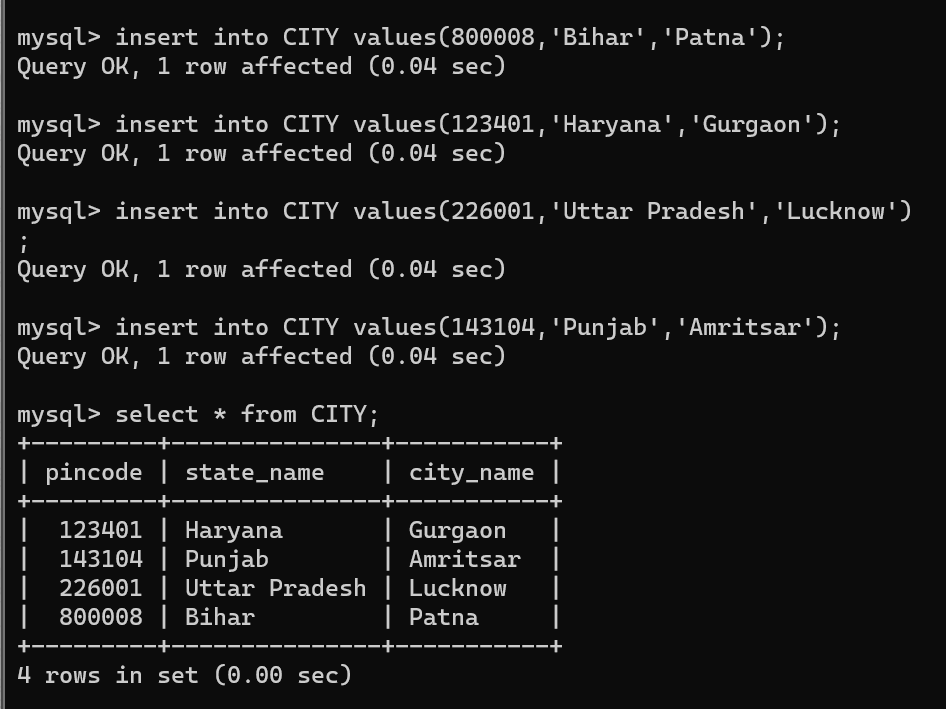
09



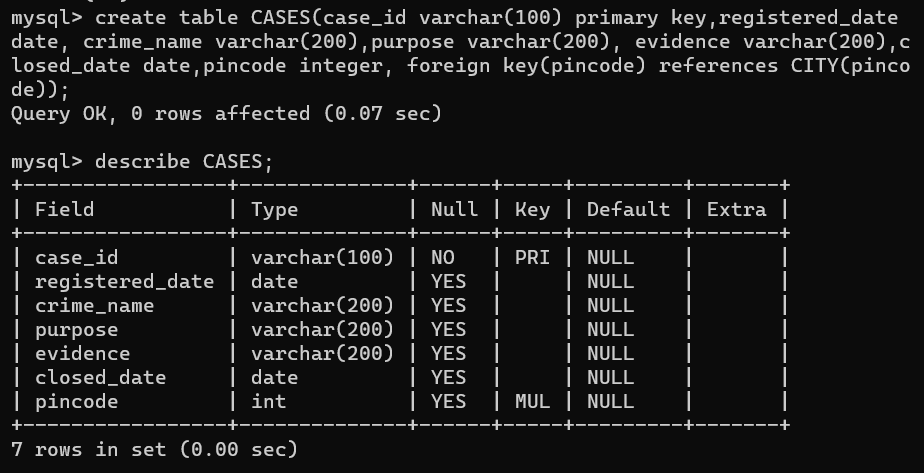
CITY (pin\_code, state\_name, city\_name)



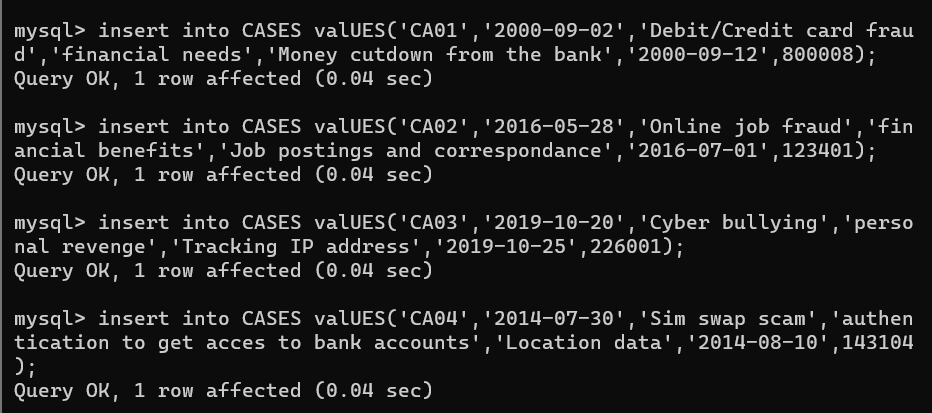
10

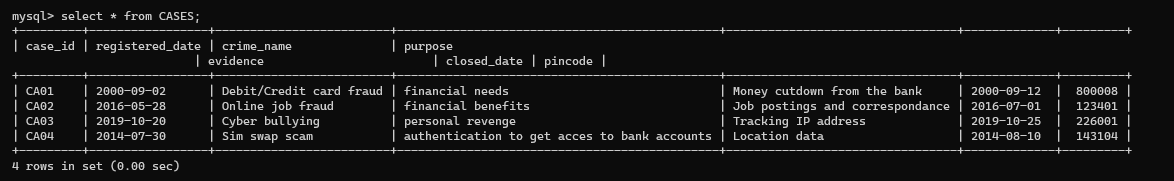


CASE (case\_id, registered\_date, crime\_name, purpose, evidence, closed\_date, pincode)

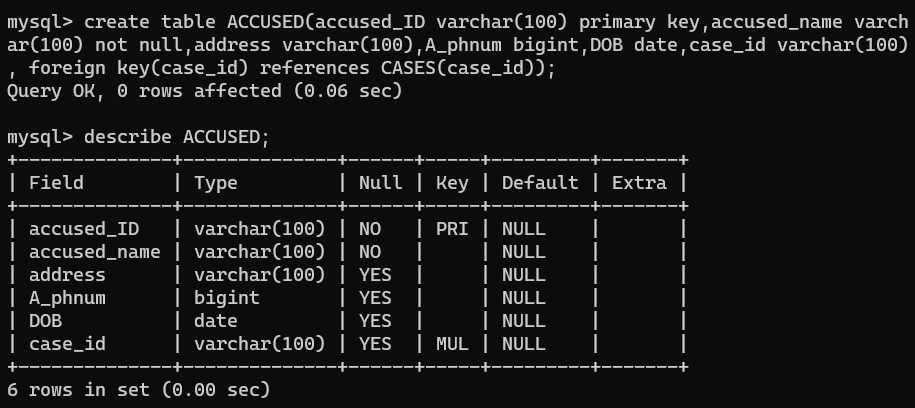


11

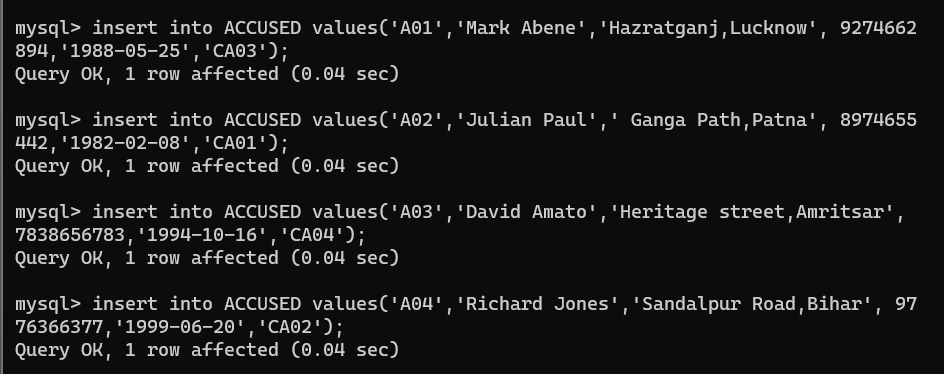


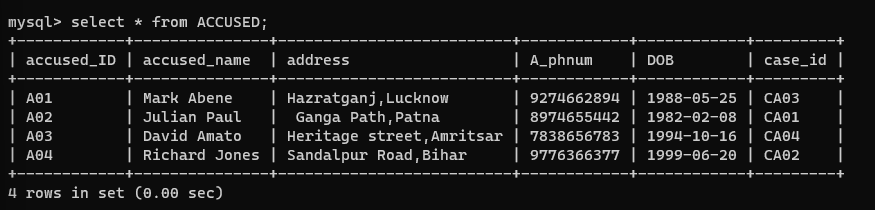


ACCUSED (accused\_id, accused\_name, address, DOB,case\_id)



12

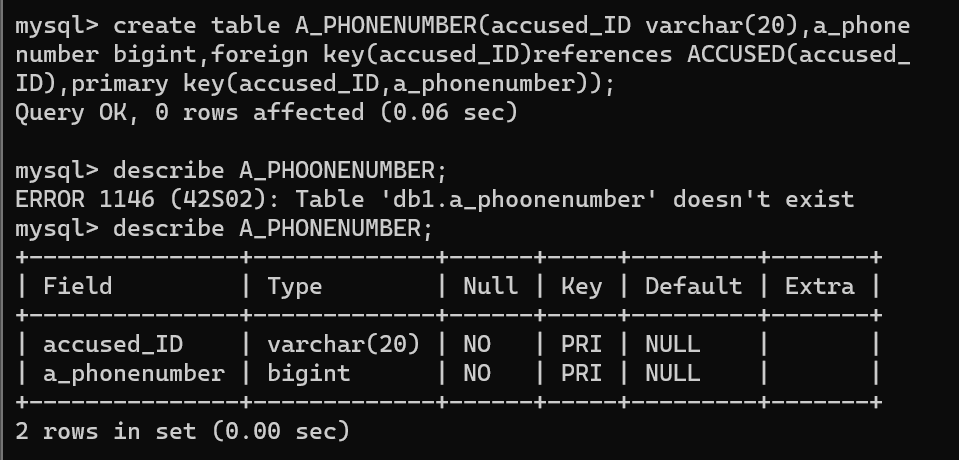


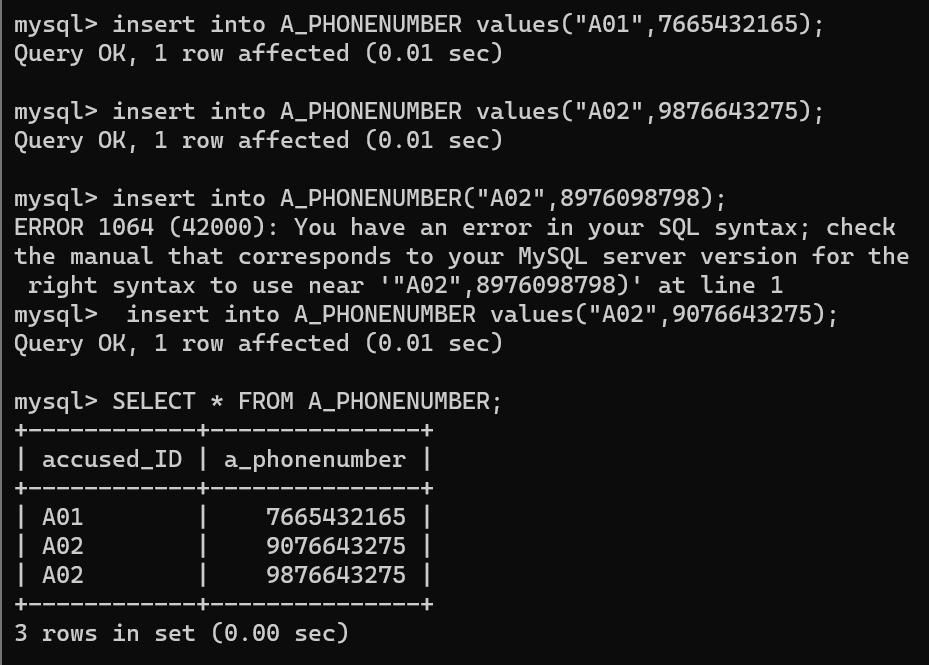




A\_PHONENUMBER (accused\_id, a\_phonenumber)

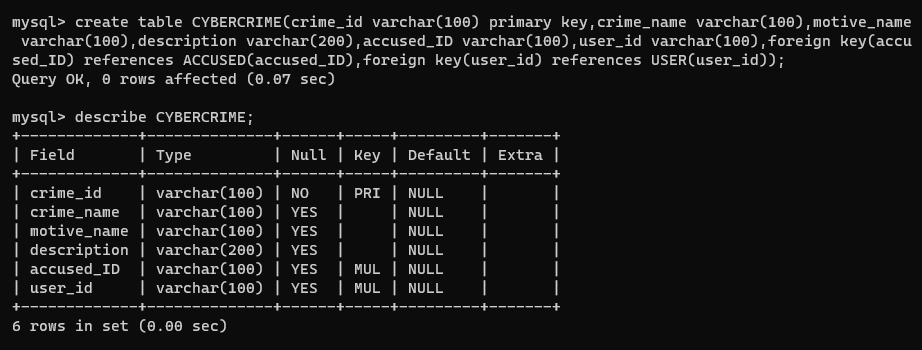
13

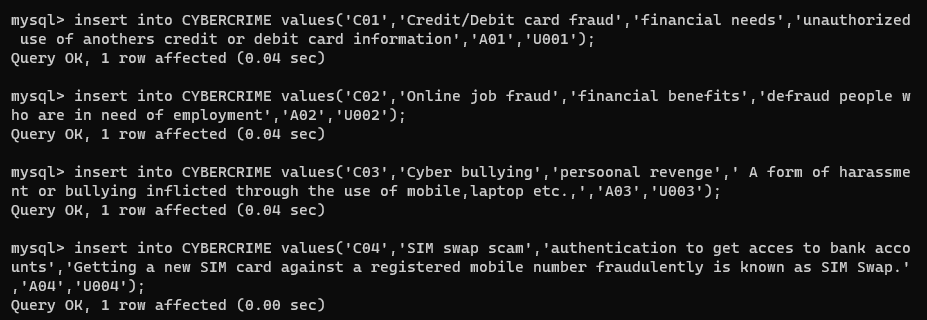


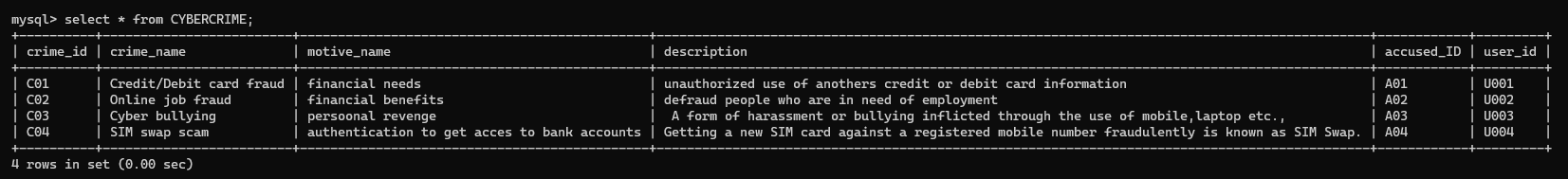


CYBERCRIME (crime\_id, crime\_name, motive\_name, description, accused\_id, user\_id)

14

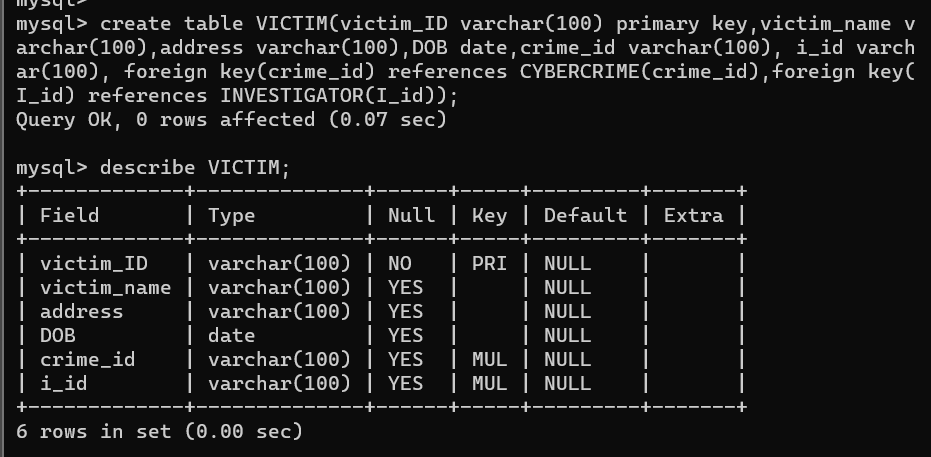


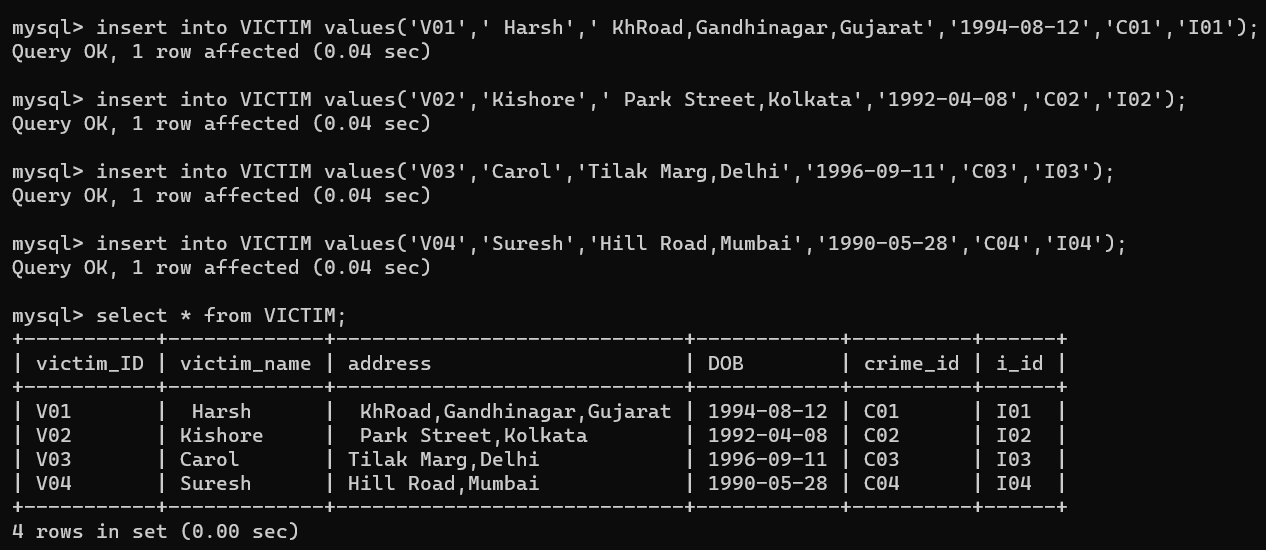




VICTIM (victim\_id, dob, address, victim\_name, crime\_id, i\_id)

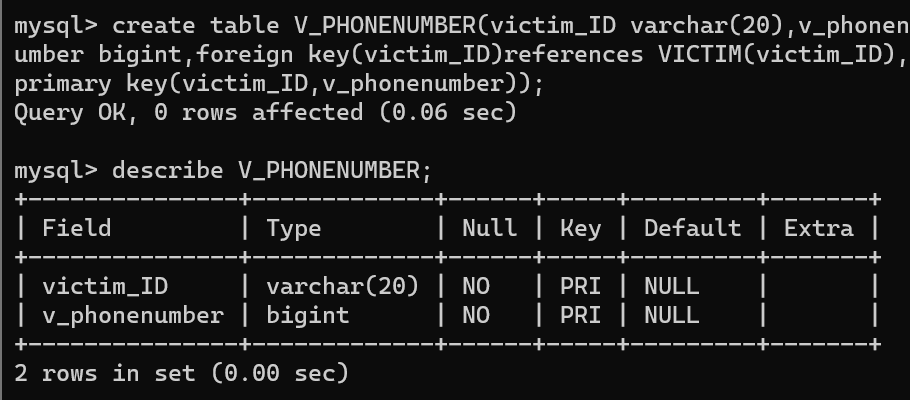
15

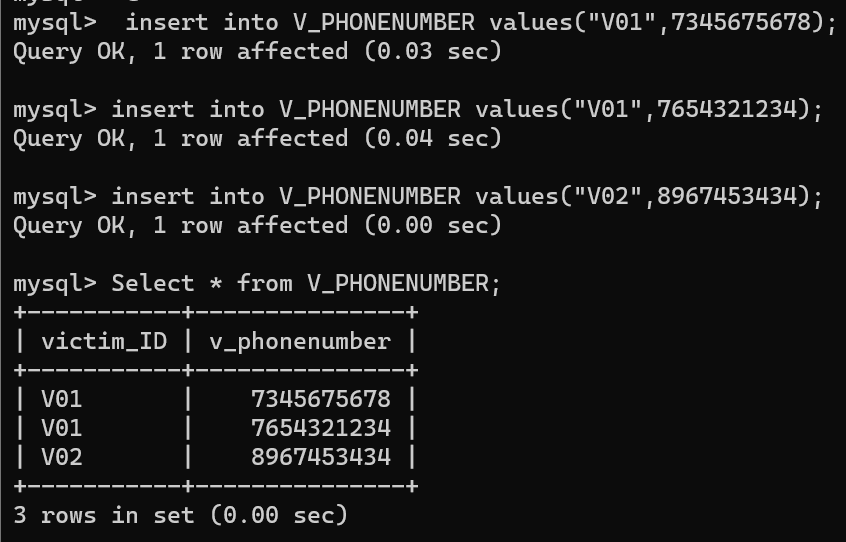




V\_PHONENUMBER (victim\_id, v\_phonenumber)

16





INVESTIGATOR (i\_id, i\_name,i\_email\_id, dept, designation)

17

