DBMS LAB REPORT
NETWORK PACKET DATABASE

SANJAY SUNIL, PES1UG21CS535
SAI SOORAJ RAMAGIRI, PES1UG21CS515

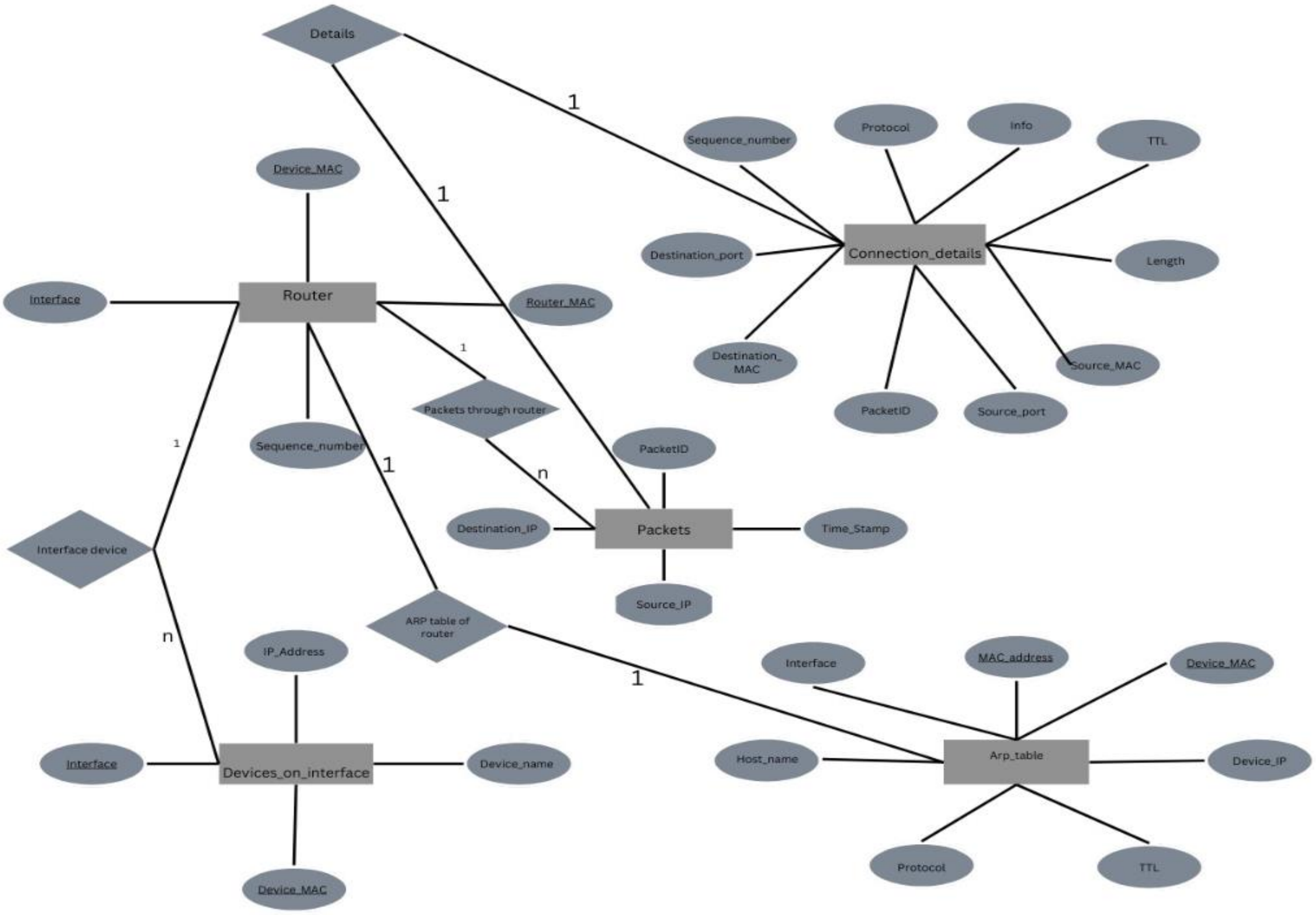
Description:

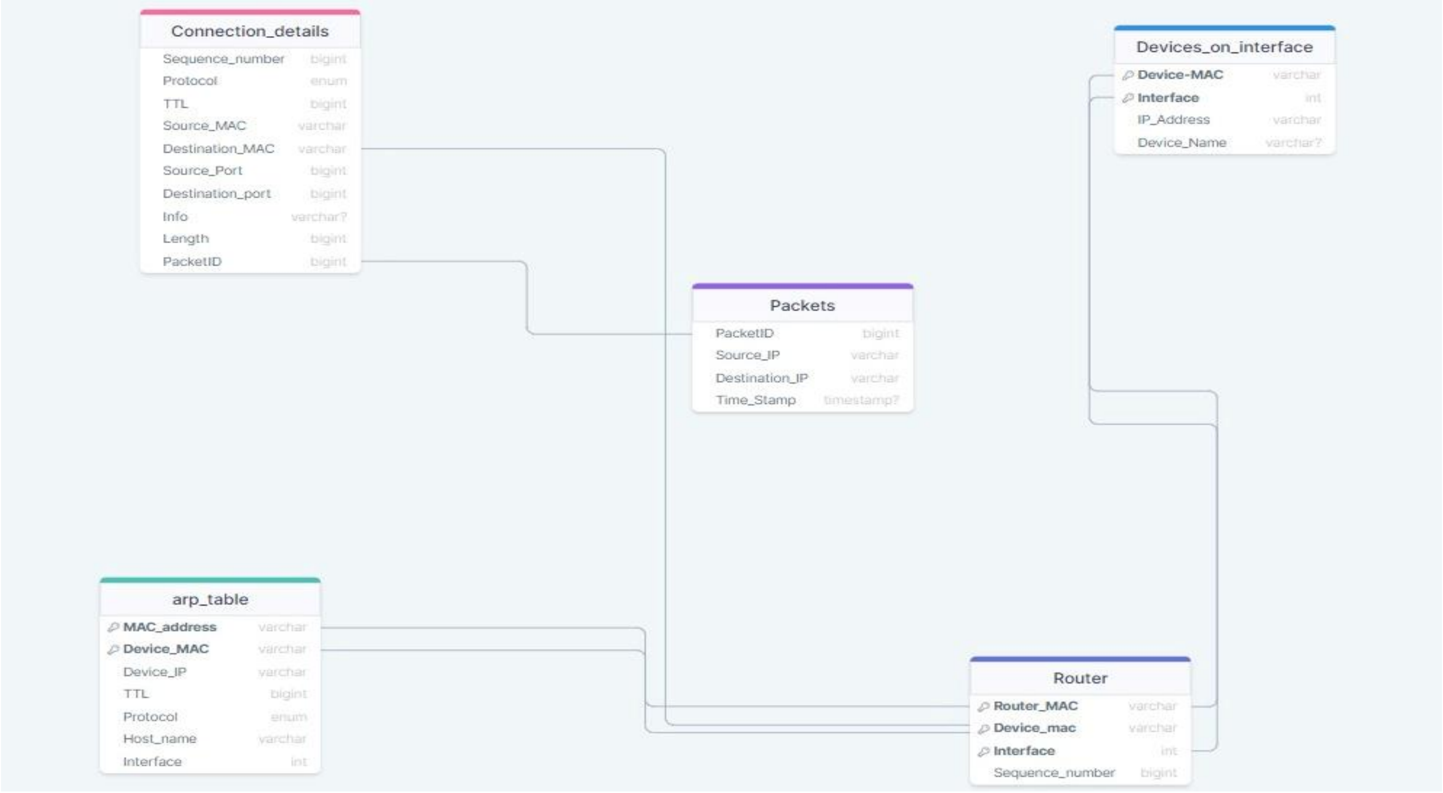
This database created is used to store information about the packets traversing a network, along with the devices and routers they encounter. The primary goal is to sense the network traffic and this can be extended to detect DDoS attacks and SYNflood attacks by just calculating dynamically, the traffic on a network regularly and matching it with unusual surging. We have demonstrated a few main examples such as packet traffic rate, interface load of packets, displaying various devices and routers linked to packets and how no one other than the database admin can alter/update/delete from a database.

Software:

We have used python, MySQL and streamlit for this project. The former 2 are for the backend, while streamlit enabled us to get a frontend local website running.

ER DIAGRAM AND SCHEMA:





Connection_details	
Sequence_number	bigint
Protocol	enum
TTL	bigint
Source_MAC	varchar
Destination_MAC	varchar
Source_Port	bigint
Destination_port	bigint
Info	varchar?
Length	bigint
PacketID	bigint

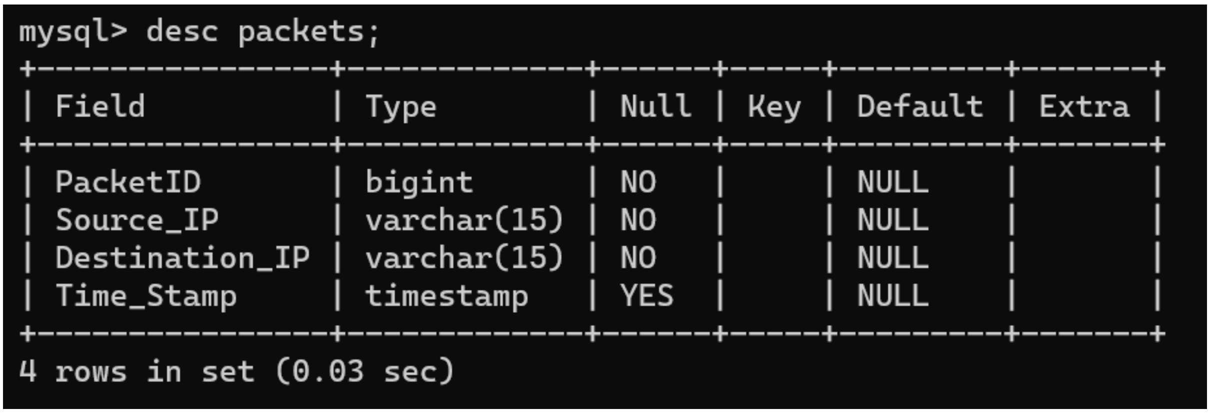
Devices_on_interface	
Device-MAC	varchar
Interface	int
IP_Address	varchar
Device_Name	varchar?

Packets	
PacketID	bigint
Source_IP	varchar
Destination_IP	varchar
Time_Stamp	timestamp?

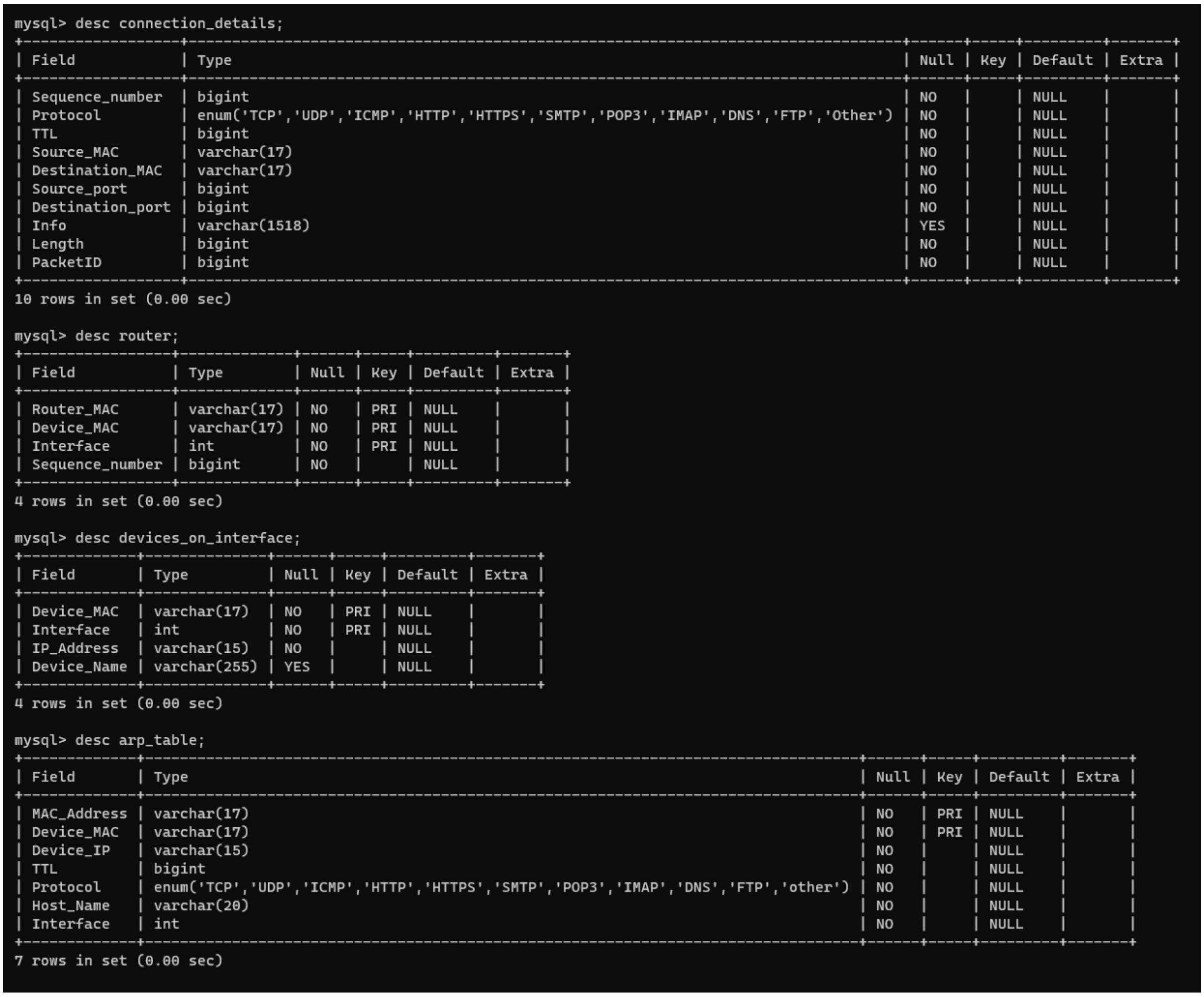
arp_table	
MAC_address	varchar
Device_MAC	varchar
Device_IP	varchar
TTL	bigint
Protocol	enum
Host_name	varchar
Interface	int

Router	
Router_MAC	varchar
Device_mac	varchar
Interface	int
Sequence_number	bigint

STRUCTURE OF TABLES:



```
mysql> desc packets;
+----------------+-------------+------+-----+---------+-------+
| Field          | Type        | Null | Key | Default | Extra |
+----------------+-------------+------+-----+---------+-------+
| PacketID       | bigint      | NO   |     | NULL    |       |
| Source_IP      | varchar(15) | NO   |     | NULL    |       |
| Destination_IP | varchar(15) | NO   |     | NULL    |       |
| Time_Stamp     | timestamp   | YES  |     | NULL    |       |
+----------------+-------------+------+-----+---------+-------+
4 rows in set (0.03 sec)
```



```
mysql> desc connection_details;
+------------------+----------------------------------------------------------------------------------+------+-----+---------+-------+
| Field            | Type                                                                             | Null | Key | Default | Extra |
+------------------+----------------------------------------------------------------------------------+------+-----+---------+-------+
| Sequence_number  | bigint                                                                           | NO   |     | NULL    |       |
| Protocol         | enum('TCP','UDP','ICMP','HTTP','HTTPS','SMTP','POP3','IMAP','DNS','FTP','Other') | NO   |     | NULL    |       |
| TTL              | bigint                                                                           | NO   |     | NULL    |       |
| Source_MAC       | varchar(17)                                                                      | NO   |     | NULL    |       |
| Destination_MAC  | varchar(17)                                                                      | NO   |     | NULL    |       |
| Source_port      | bigint                                                                           | NO   |     | NULL    |       |
| Destination_port | bigint                                                                           | NO   |     | NULL    |       |
| Info             | varchar(1518)                                                                    | YES  |     | NULL    |       |
| Length           | bigint                                                                           | NO   |     | NULL    |       |
| PacketID         | bigint                                                                           | NO   |     | NULL    |       |
+------------------+----------------------------------------------------------------------------------+------+-----+---------+-------+
10 rows in set (0.00 sec)

mysql> desc router;
+-----------------+-------------+------+-----+---------+-------+
| Field           | Type        | Null | Key | Default | Extra |
+-----------------+-------------+------+-----+---------+-------+
| Router_MAC      | varchar(17) | NO   | PRI | NULL    |       |
| Device_MAC      | varchar(17) | NO   | PRI | NULL    |       |
| Interface       | int         | NO   | PRI | NULL    |       |
| Sequence_number | bigint      | NO   |     | NULL    |       |
+-----------------+-------------+------+-----+---------+-------+
4 rows in set (0.00 sec)

mysql> desc devices_on_interface;
+-------------+--------------+------+-----+---------+-------+
| Field       | Type         | Null | Key | Default | Extra |
+-------------+--------------+------+-----+---------+-------+
| Device_MAC  | varchar(17)  | NO   | PRI | NULL    |       |
| Interface   | int          | NO   | PRI | NULL    |       |
| IP_Address  | varchar(15)  | NO   |     | NULL    |       |
| Device_Name | varchar(255) | YES  |     | NULL    |       |
+-------------+--------------+------+-----+---------+-------+
4 rows in set (0.00 sec)

mysql> desc arp_table;
+-------------+----------------------------------------------------------------------------------+------+-----+---------+-------+
| Field       | Type                                                                             | Null | Key | Default | Extra |
+-------------+----------------------------------------------------------------------------------+------+-----+---------+-------+
| MAC_Address | varchar(17)                                                                      | NO   | PRI | NULL    |       |
| Device_MAC  | varchar(17)                                                                      | NO   | PRI | NULL    |       |
| Device_IP   | varchar(15)                                                                      | NO   |     | NULL    |       |
| TTL         | bigint                                                                           | NO   |     | NULL    |       |
| Protocol    | enum('TCP','UDP','ICMP','HTTP','HTTPS','SMTP','POP3','IMAP','DNS','FTP','other') | NO   |     | NULL    |       |
| Host_Name   | varchar(20)                                                                      | NO   |     | NULL    |       |
| Interface   | int                                                                              | NO   |     | NULL    |       |
+-------------+----------------------------------------------------------------------------------+------+-----+---------+-------+
7 rows in set (0.00 sec)
```

- The database consists of four main tables: packets, connection_details, router, and devices_on_interface, each designed to store specific information related to network communication and device connectivity.

- The packets table captures packet level details, including PacketID, source and destination IP addresses, and a timestamp, providing a granular view of network traffic.

- The connection_details table contains information about network connections, such as sequence number, protocol type, Time To Live (TTL), source and destination MAC addresses, ports, packet length, and additional information.

- The router table maintains data about routers, with Router_MAC, Device_MAC, Interface, and Sequence_number fields, facilitating the organization and management of routing devices in the network.

- The arp_table table focuses on Address Resolution Protocol (ARP) details, featuring MAC_Address, Device_MAC, Device_IP, TTL, protocol type, host name, and interface fields, offering insights into device connectivity and address resolution within the network.

LINKS

- Linkage between packets and connection_details: Both tables have a common field named PacketID, which serves as a foreign key in the connection_details table, linking each connection detail entry to a specific packet in the packets table.

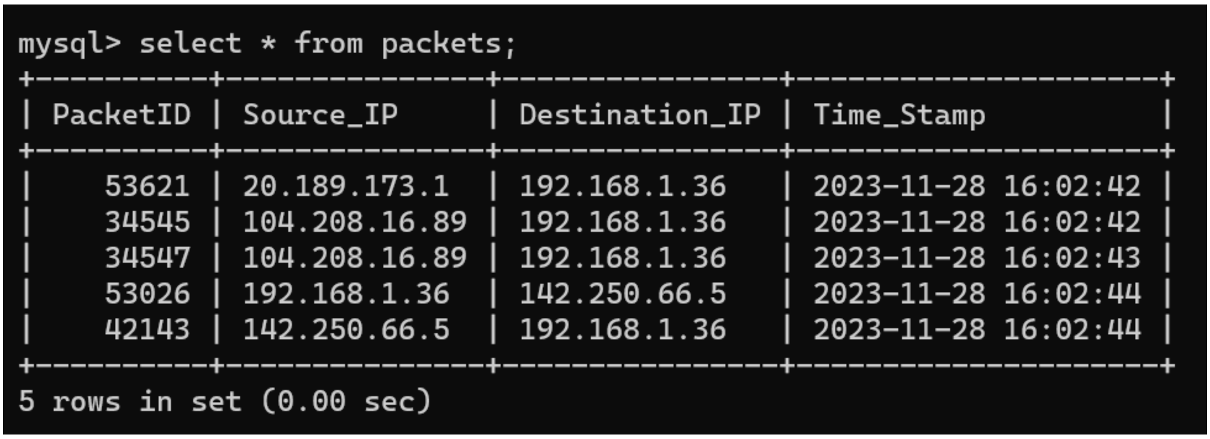
- Linkage between connection_details and router: The connection_details table contains a field named Sequence_number, which serves as a foreign key in the router table, linking each router entry to a specific connection detail.

- Linkage between devices_on_interface and router: The devices_on_interface table has two fields, Device_MAC and Interface, serving as foreign keys that link to the Router_MAC and Interface fields in the router table. This linkage establishes the relationship between devices connected to specific router interfaces.

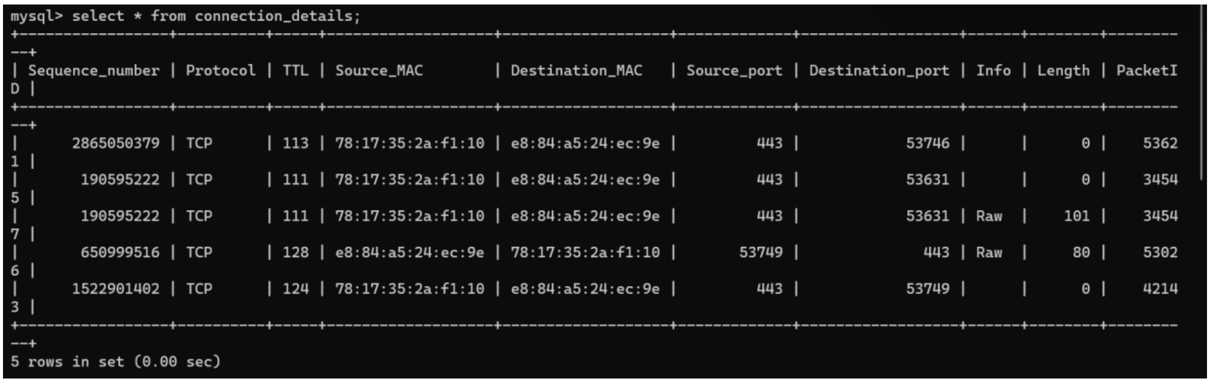
- Linkage between arp_table and devices_on_interface: The arp_table table has a field named Device_MAC, which is a foreign key linking to the Device_MAC field in the devices_on_interface table. This linkage connects ARP details to specific devices on interfaces.

- Linkage between arp_table and router: The arp_table table also contains an Interface field, serving as a foreign key that links to the Interface field in the router table. This linkage associates ARP details with specific router interfaces.

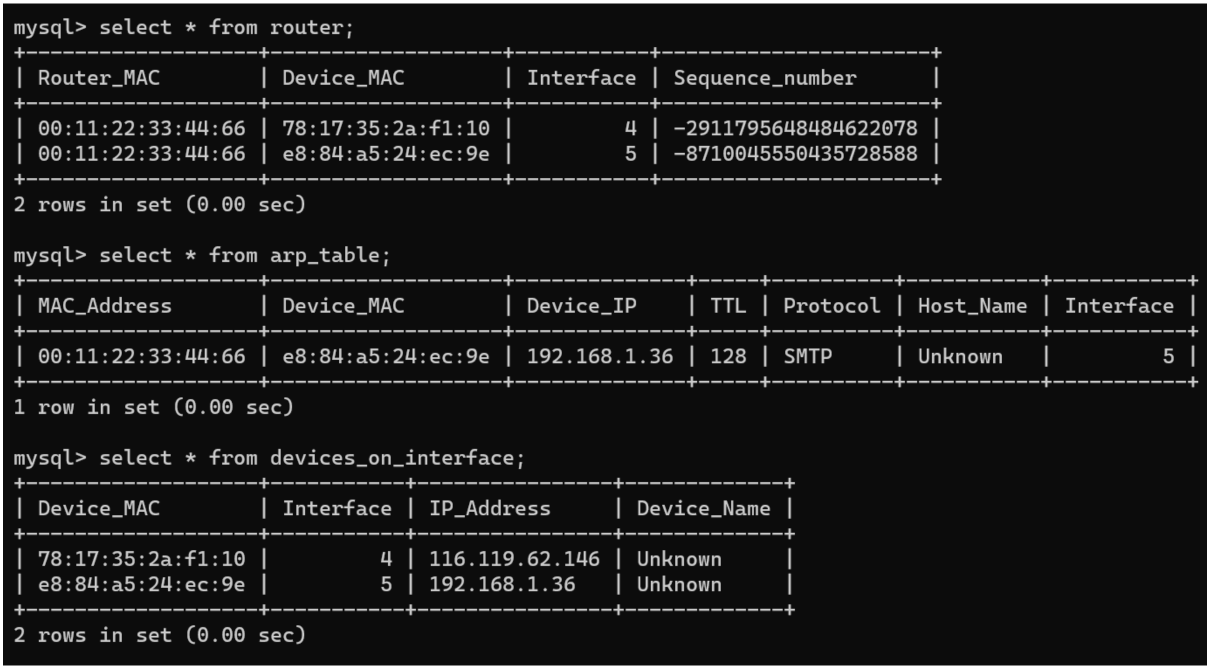
Content of the DB after executing the code which we have put up after the output:



```
mysql> select * from packets;
+----------+---------------+----------------+---------------------+
| PacketID | Source_IP     | Destination_IP | Time_Stamp          |
+----------+---------------+----------------+---------------------+
|    53621 | 20.189.173.1  | 192.168.1.36   | 2023-11-28 16:02:42 |
|    34545 | 104.208.16.89 | 192.168.1.36   | 2023-11-28 16:02:42 |
|    34547 | 104.208.16.89 | 192.168.1.36   | 2023-11-28 16:02:43 |
|    53026 | 192.168.1.36  | 142.250.66.5   | 2023-11-28 16:02:44 |
|    42143 | 142.250.66.5  | 192.168.1.36   | 2023-11-28 16:02:44 |
+----------+---------------+----------------+---------------------+
5 rows in set (0.00 sec)
```

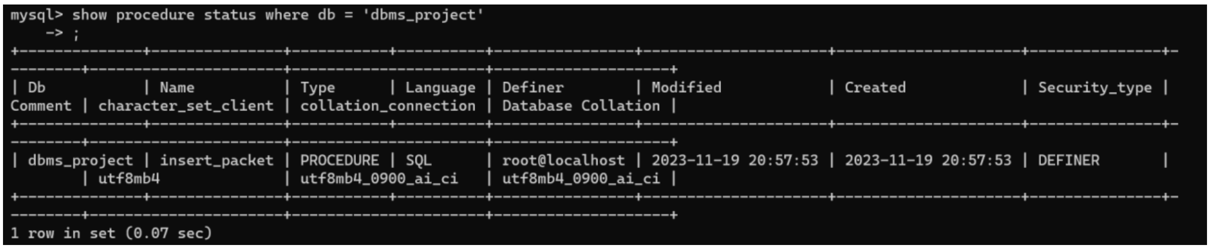


```
mysql> select * from connection_details;
+-----------------+----------+-----+-------------------+-------------------+-------------+------------------+------+--------+--------
--+
| Sequence_number | Protocol | TTL | Source_MAC        | Destination_MAC   | Source_port | Destination_port | Info | Length | PacketI
D |
+-----------------+----------+-----+-------------------+-------------------+-------------+------------------+------+--------+--------
--+
|      2865050379 | TCP      | 113 | 78:17:35:2a:f1:10 | e8:84:a5:24:ec:9e |         443 |            53746 |      |      0 |    5362
1 |
|       190595222 | TCP      | 111 | 78:17:35:2a:f1:10 | e8:84:a5:24:ec:9e |         443 |            53631 |      |      0 |    3454
5 |
|       190595222 | TCP      | 111 | 78:17:35:2a:f1:10 | e8:84:a5:24:ec:9e |         443 |            53631 | Raw  |    101 |    3454
7 |
|       650999516 | TCP      | 128 | e8:84:a5:24:ec:9e | 78:17:35:2a:f1:10 |       53749 |              443 | Raw  |     80 |    5302
6 |
|      1522901402 | TCP      | 124 | 78:17:35:2a:f1:10 | e8:84:a5:24:ec:9e |         443 |            53749 |      |      0 |    4214
3 |
+-----------------+----------+-----+-------------------+-------------------+-------------+------------------+------+--------+--------
--+
5 rows in set (0.00 sec)
```

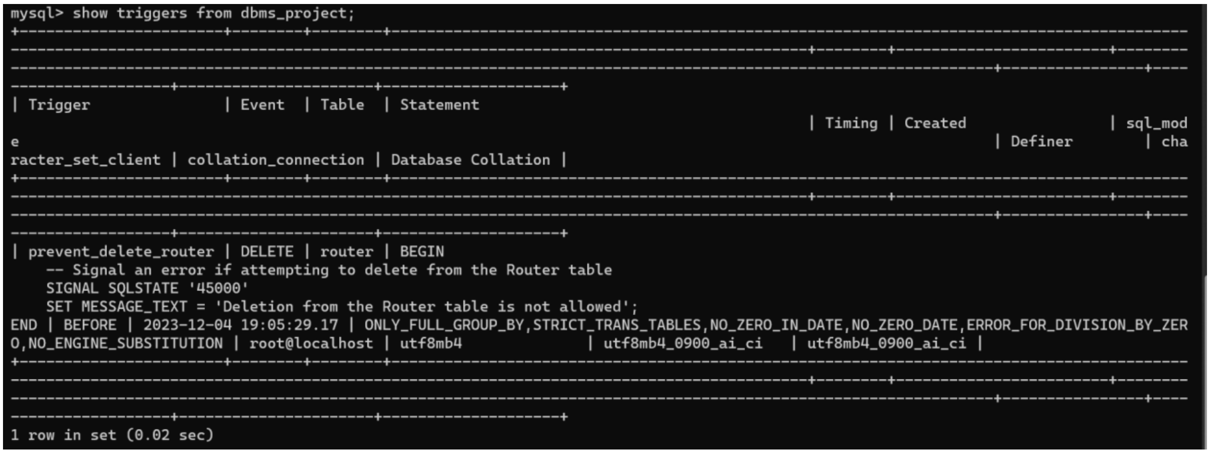


```
mysql> select * from router;
+-------------------+-------------------+-----------+----------------------+
| Router_MAC        | Device_MAC        | Interface | Sequence_number      |
+-------------------+-------------------+-----------+----------------------+
| 00:11:22:33:44:66 | 78:17:35:2a:f1:10 |         4 | -2911795648484622078 |
| 00:11:22:33:44:66 | e8:84:a5:24:ec:9e |         5 | -8710045550435728588 |
+-------------------+-------------------+-----------+----------------------+
2 rows in set (0.00 sec)

mysql> select * from arp_table;
+-------------------+-------------------+--------------+-----+----------+-----------+-----------+
| MAC_Address       | Device_MAC        | Device_IP    | TTL | Protocol | Host_Name | Interface |
+-------------------+-------------------+--------------+-----+----------+-----------+-----------+
| 00:11:22:33:44:66 | e8:84:a5:24:ec:9e | 192.168.1.36 | 128 | SMTP     | Unknown   |         5 |
+-------------------+-------------------+--------------+-----+----------+-----------+-----------+
1 row in set (0.00 sec)

mysql> select * from devices_on_interface;
+-------------------+-----------+----------------+-------------+
| Device_MAC        | Interface | IP_Address     | Device_Name |
+-------------------+-----------+----------------+-------------+
| 78:17:35:2a:f1:10 |         4 | 116.119.62.146 | Unknown     |
| e8:84:a5:24:ec:9e |         5 | 192.168.1.36   | Unknown     |
+-------------------+-----------+----------------+-------------+
2 rows in set (0.00 sec)
```

TRIGGERS AND PROCEDURES USED:

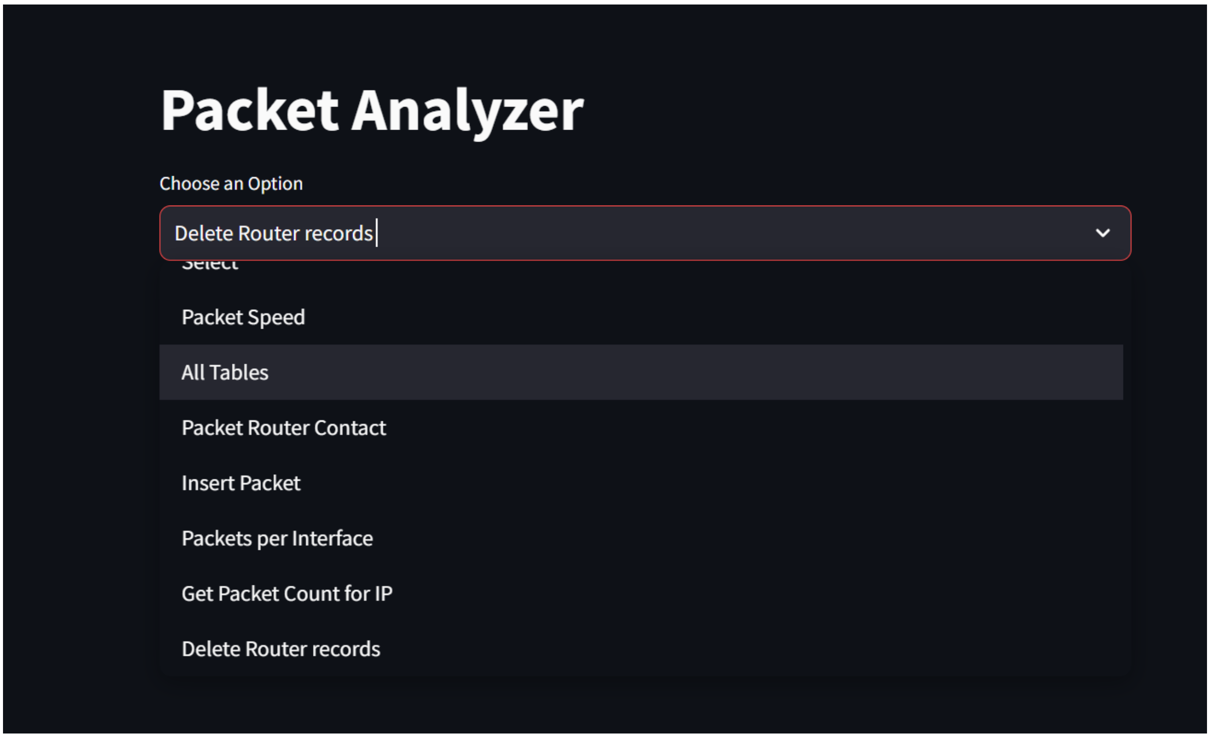


```
mysql> show procedure status where db = 'dbms_project'
    -> ;
+-------------+---------------+-----------+----------+----------------+---------------------+---------------------+---------------+-
--------+----------------------+----------------------+--------------------+
| Db          | Name          | Type      | Language | Definer        | Modified            | Created             | Security_type |
Comment | character_set_client | collation_connection | Database Collation |
+-------------+---------------+-----------+----------+----------------+---------------------+---------------------+---------------+-
--------+----------------------+----------------------+--------------------+
| dbms_project | insert_packet | PROCEDURE | SQL      | root@localhost | 2023-11-19 20:57:53 | 2023-11-19 20:57:53 | DEFINER       |
        | utf8mb4              | utf8mb4_0900_ai_ci   | utf8mb4_0900_ai_ci |
+-------------+---------------+-----------+----------+----------------+---------------------+---------------------+---------------+-
--------+----------------------+----------------------+--------------------+
1 row in set (0.07 sec)
```



```
mysql> show triggers from dbms_project;
+-----------------------+--------+--------+-----------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------+--------+------------------------+--------
----------------------------------------------------------------------------------------------------------------+-----------------+----
-----------------+----------------------+--------------------+
| Trigger               | Event  | Table  | Statement
                                                                                           | Timing | Created                | sql_mod
e                                                                                                                | Definer         | cha
racter_set_client | collation_connection | Database Collation |
+-----------------------+--------+--------+-----------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------+--------+------------------------+--------
----------------------------------------------------------------------------------------------------------------+-----------------+----
-----------------+----------------------+--------------------+
| prevent_delete_router | DELETE | router | BEGIN
    -- Signal an error if attempting to delete from the Router table
    SIGNAL SQLSTATE '45000'
    SET MESSAGE_TEXT = 'Deletion from the Router table is not allowed';
END | BEFORE | 2023-12-04 19:05:29.17 | ONLY_FULL_GROUP_BY,STRICT_TRANS_TABLES,NO_ZERO_IN_DATE,NO_ZERO_DATE,ERROR_FOR_DIVISION_BY_ZER
O,NO_ENGINE_SUBSTITUTION | root@localhost | utf8mb4              | utf8mb4_0900_ai_ci   | utf8mb4_0900_ai_ci |
+-----------------------+--------+--------+-----------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------+--------+------------------------+--------
----------------------------------------------------------------------------------------------------------------+-----------------+----
-----------------+----------------------+--------------------+
1 row in set (0.02 sec)
```

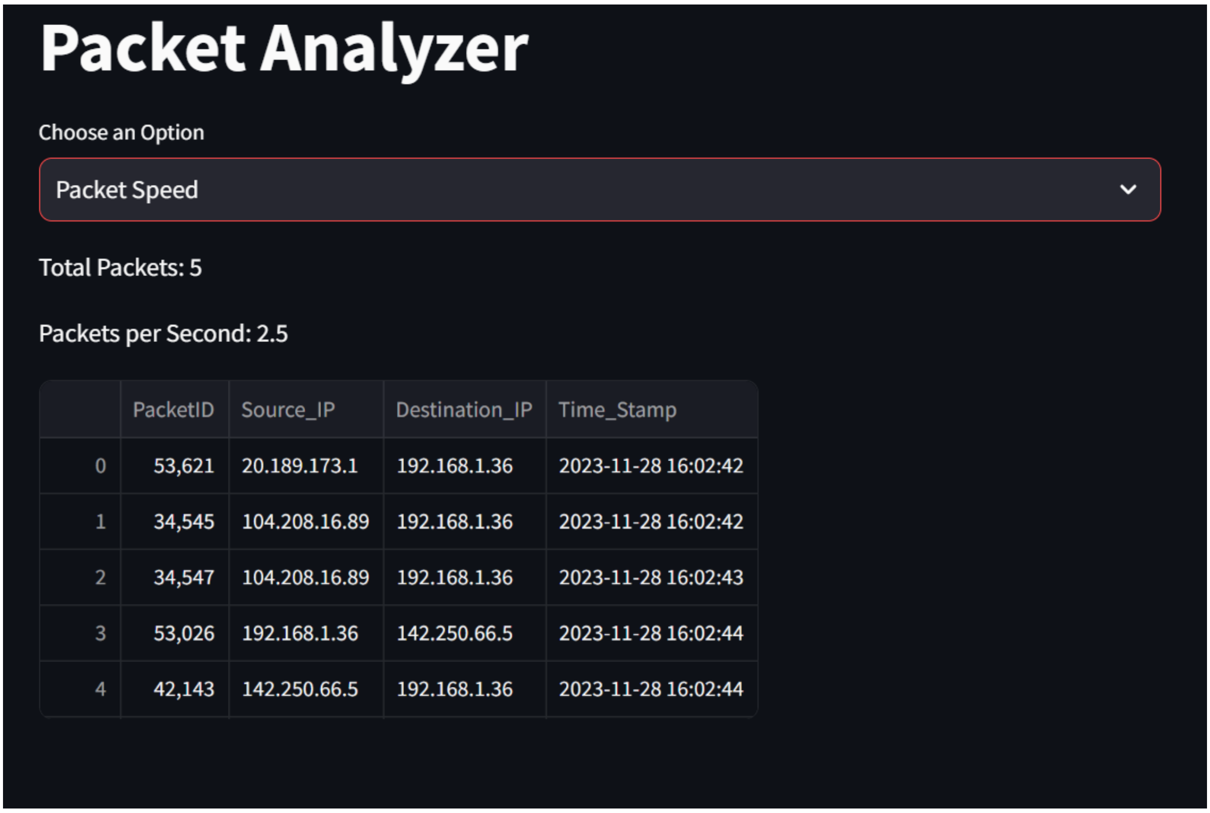
FRONTEND:



Packet Analyzer

Choose an Option: Delete Router records

7 options as seen above



Packet Analyzer

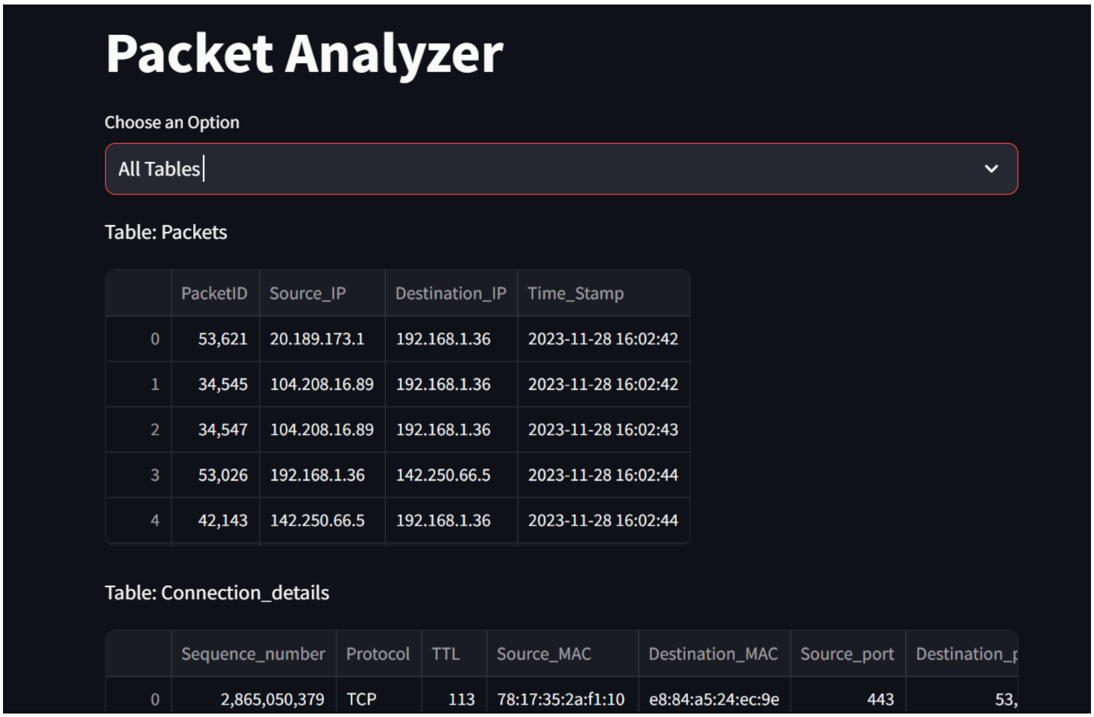
Choose an Option: Packet Speed

Total Packets: 5

Packets per Second: 2.5

	PacketID	Source_IP	Destination_IP	Time_Stamp
0	53,621	20.189.173.1	192.168.1.36	2023-11-28 16:02:42
1	34,545	104.208.16.89	192.168.1.36	2023-11-28 16:02:42
2	34,547	104.208.16.89	192.168.1.36	2023-11-28 16:02:43
3	53,026	192.168.1.36	142.250.66.5	2023-11-28 16:02:44
4	42,143	142.250.66.5	192.168.1.36	2023-11-28 16:02:44

This computes the packet speed based on the first and last timestamps of packet table entries.



Packet Analyzer

Choose an Option

All Tables

Table: Packets

	PacketID	Source_IP	Destination_IP	Time_Stamp
0	53,621	20.189.173.1	192.168.1.36	2023-11-28 16:02:42
1	34,545	104.208.16.89	192.168.1.36	2023-11-28 16:02:42
2	34,547	104.208.16.89	192.168.1.36	2023-11-28 16:02:43
3	53,026	192.168.1.36	142.250.66.5	2023-11-28 16:02:44
4	42,143	142.250.66.5	192.168.1.36	2023-11-28 16:02:44

Table: Connection_details

	Sequence_number	Protocol	TTL	Source_MAC	Destination_MAC	Source_port	Destination_p
0	2,865,050,379	TCP	113	78:17:35:2a:f1:10	e8:84:a5:24:ec:9e	443	53,

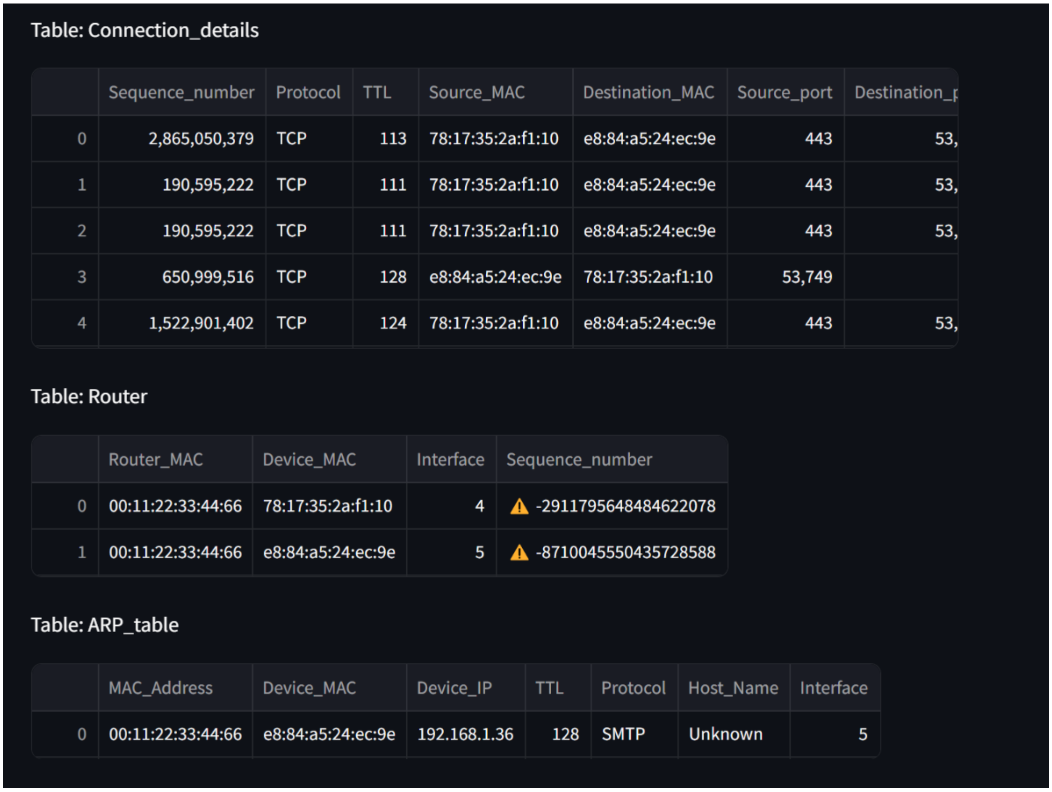


Table: Connection_details

	Sequence_number	Protocol	TTL	Source_MAC	Destination_MAC	Source_port	Destination_p
0	2,865,050,379	TCP	113	78:17:35:2a:f1:10	e8:84:a5:24:ec:9e	443	53,
1	190,595,222	TCP	111	78:17:35:2a:f1:10	e8:84:a5:24:ec:9e	443	53,
2	190,595,222	TCP	111	78:17:35:2a:f1:10	e8:84:a5:24:ec:9e	443	53,
3	650,999,516	TCP	128	e8:84:a5:24:ec:9e	78:17:35:2a:f1:10	53,749	
4	1,522,901,402	TCP	124	78:17:35:2a:f1:10	e8:84:a5:24:ec:9e	443	53,

Table: Router

	Router_MAC	Device_MAC	Interface	Sequence_number
0	00:11:22:33:44:66	78:17:35:2a:f1:10	4	⚠ -2911795648484622078
1	00:11:22:33:44:66	e8:84:a5:24:ec:9e	5	⚠ -8710045550435728588

Table: ARP_table

	MAC_Address	Device_MAC	Device_IP	TTL	Protocol	Host_Name	Interface
0	00:11:22:33:44:66	e8:84:a5:24:ec:9e	192.168.1.36	128	SMTP	Unknown	5

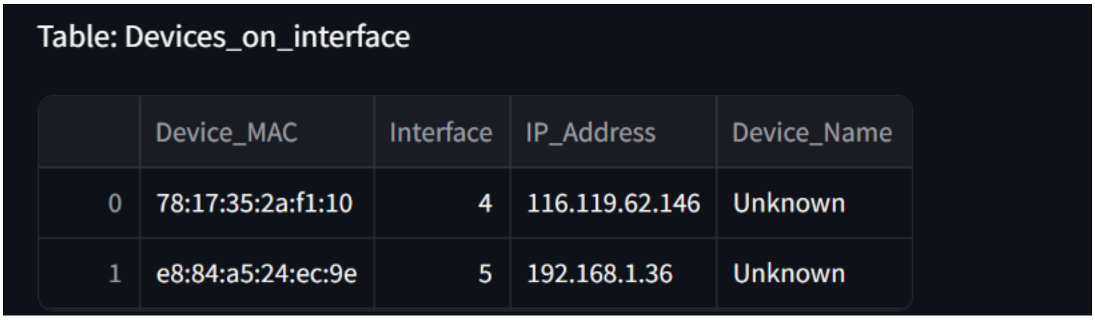
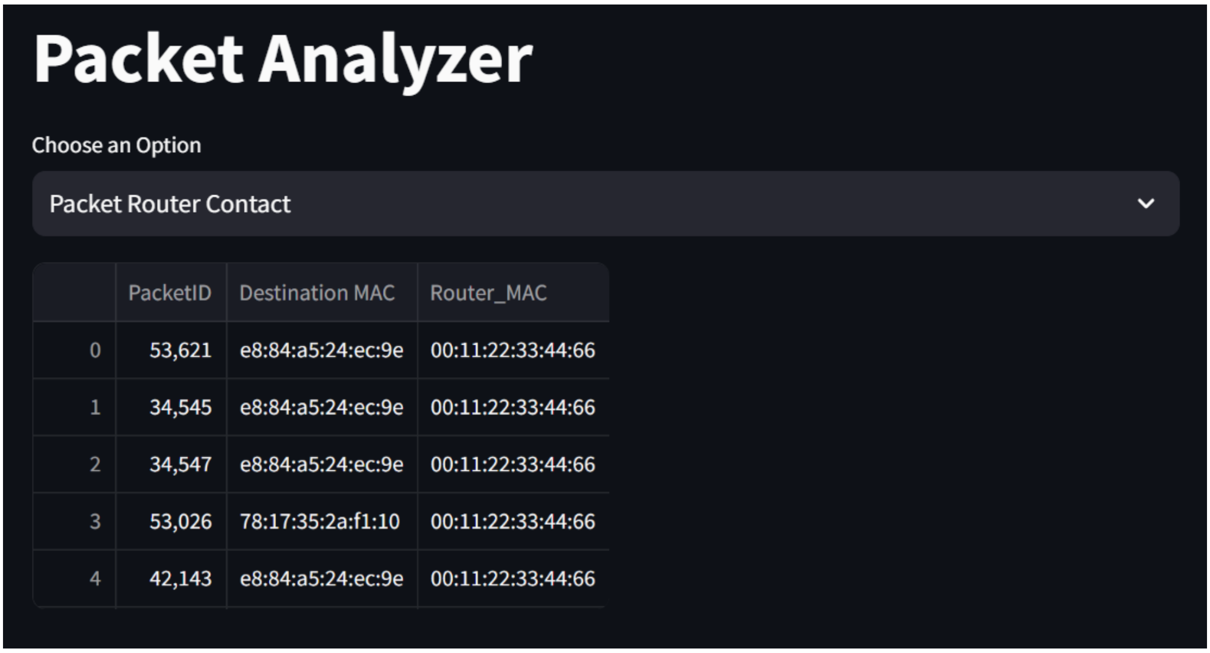


Table: Devices_on_interface

	Device_MAC	Interface	IP_Address	Device_Name
0	78:17:35:2a:f1:10	4	116.119.62.146	Unknown
1	e8:84:a5:24:ec:9e	5	192.168.1.36	Unknown

All the tables are displayed.

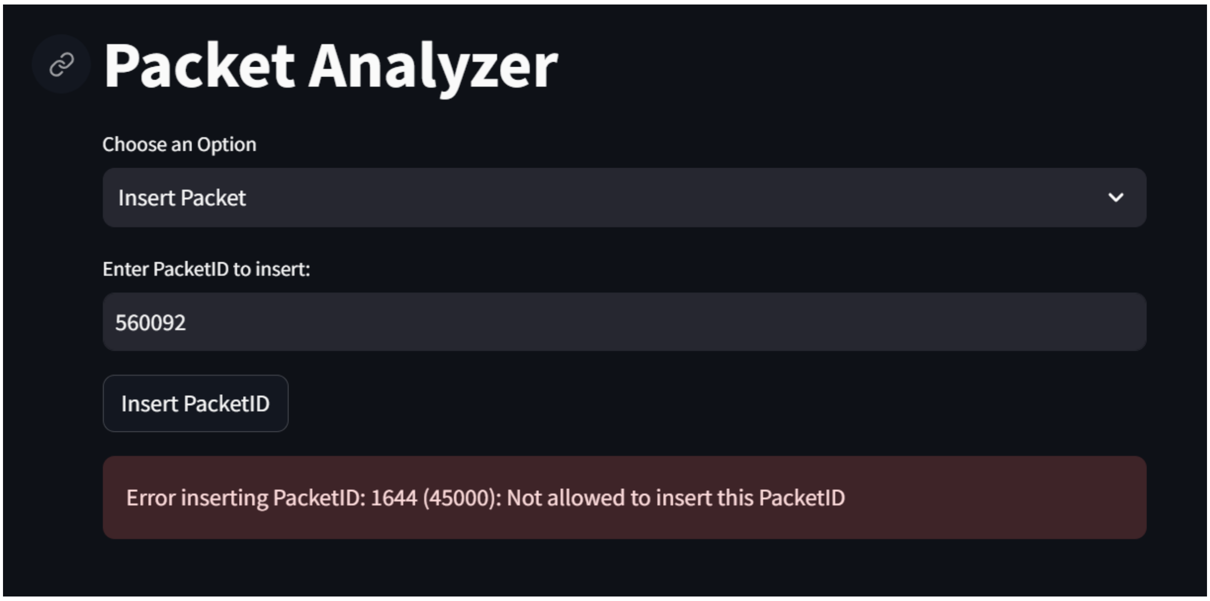


Packet Analyzer

Choose an Option: Packet Router Contact

	PacketID	Destination MAC	Router_MAC
0	53,621	e8:84:a5:24:ec:9e	00:11:22:33:44:66
1	34,545	e8:84:a5:24:ec:9e	00:11:22:33:44:66
2	34,547	e8:84:a5:24:ec:9e	00:11:22:33:44:66
3	53,026	78:17:35:2a:f1:10	00:11:22:33:44:66
4	42,143	e8:84:a5:24:ec:9e	00:11:22:33:44:66

Displays the packets and the routers they pass through along with the device MAC addresses.



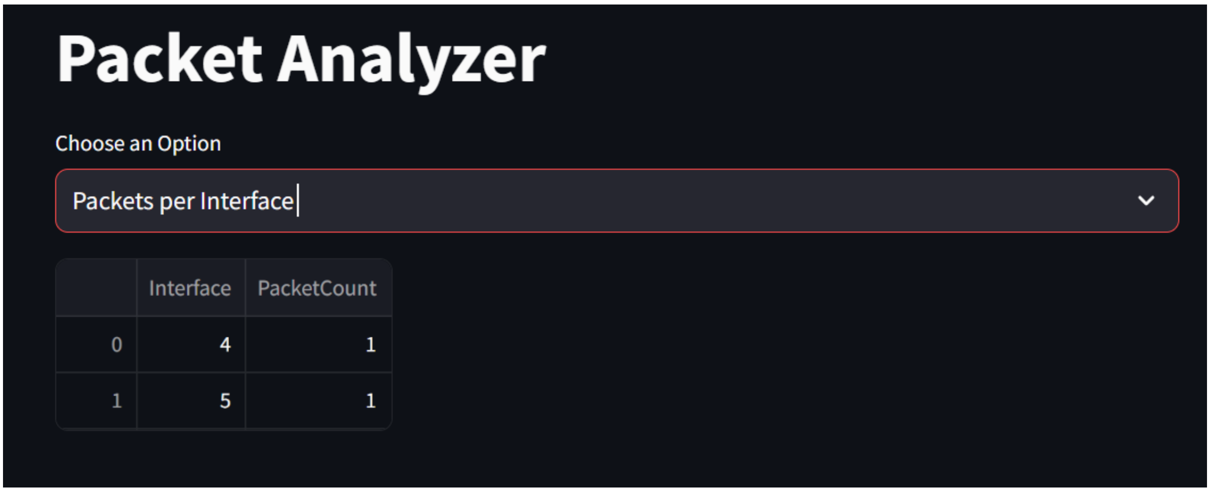
Packet Analyzer

Choose an Option: Insert Packet

Enter PacketID to insert: 560092

Error inserting PacketID: 1644 (45000): Not allowed to insert this PacketID

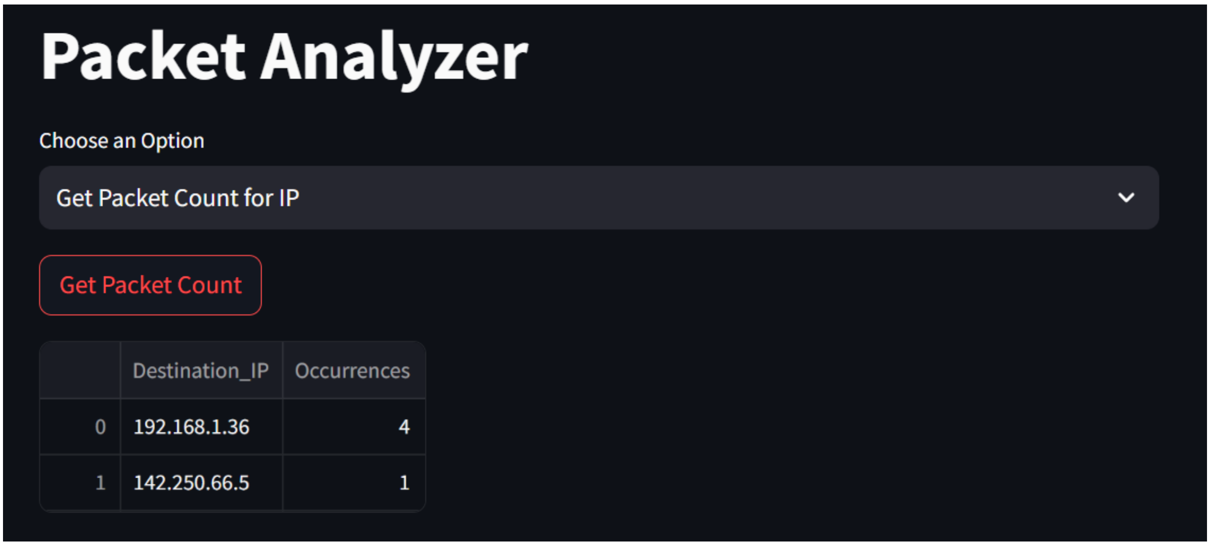
A procedure has been defined to prevent the addition of packets by anyone logged in other than the admin.



Packet Analyzer

Choose an Option: Packets per Interface

	Interface	PacketCount
0	4	1
1	5	1

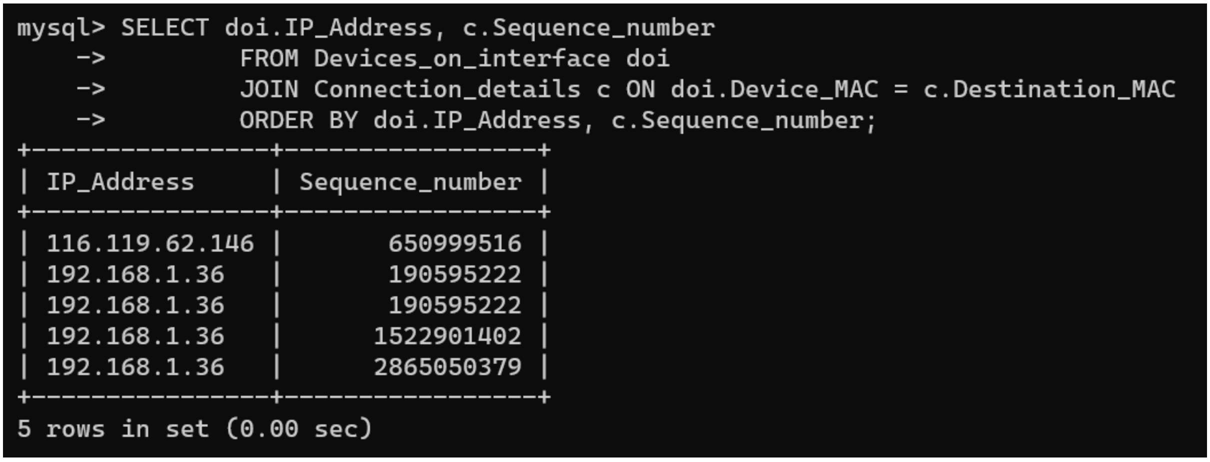


Packet Analyzer

Choose an Option

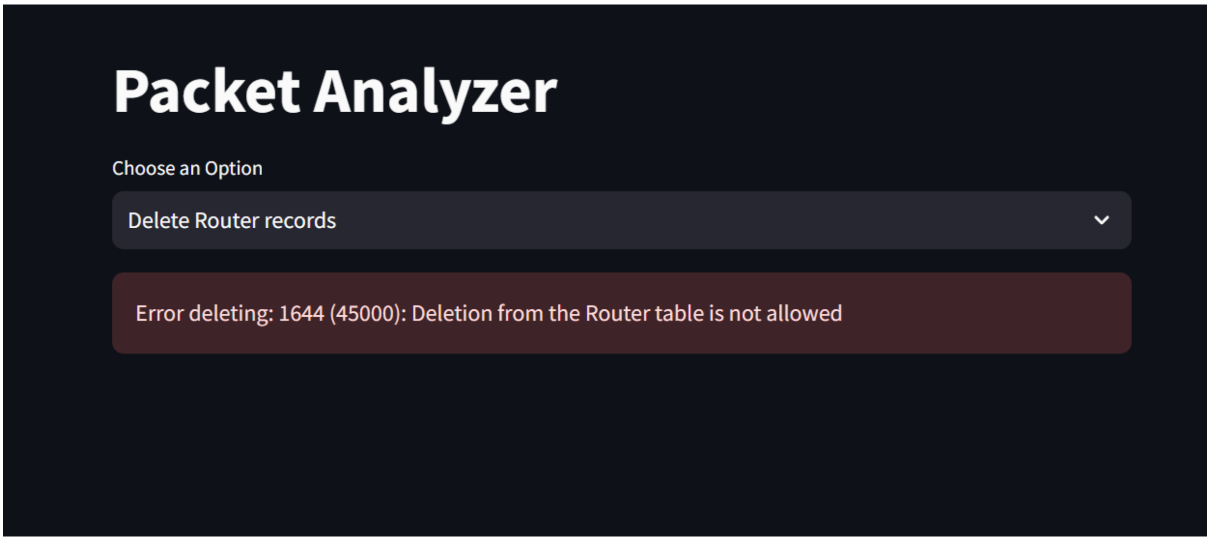
Get Packet Count for IP

	Destination_IP	Occurrences
0	192.168.1.36	4
1	142.250.66.5	1



```
mysql> SELECT doi.IP_Address, c.Sequence_number
    ->         FROM Devices_on_interface doi
    ->         JOIN Connection_details c ON doi.Device_MAC = c.Destination_MAC
    ->         ORDER BY doi.IP_Address, c.Sequence_number;
+----------------+-----------------+
| IP_Address     | Sequence_number |
+----------------+-----------------+
| 116.119.62.146 |       650999516 |
| 192.168.1.36   |       190595222 |
| 192.168.1.36   |       190595222 |
| 192.168.1.36   |      1522901402 |
| 192.168.1.36   |      2865050379 |
+----------------+-----------------+
5 rows in set (0.00 sec)
```

We had plans to display the packets and to which IP addresses they are going to. Unfortunately, this wasn’t being displayed on the front end.



Packet Analyzer

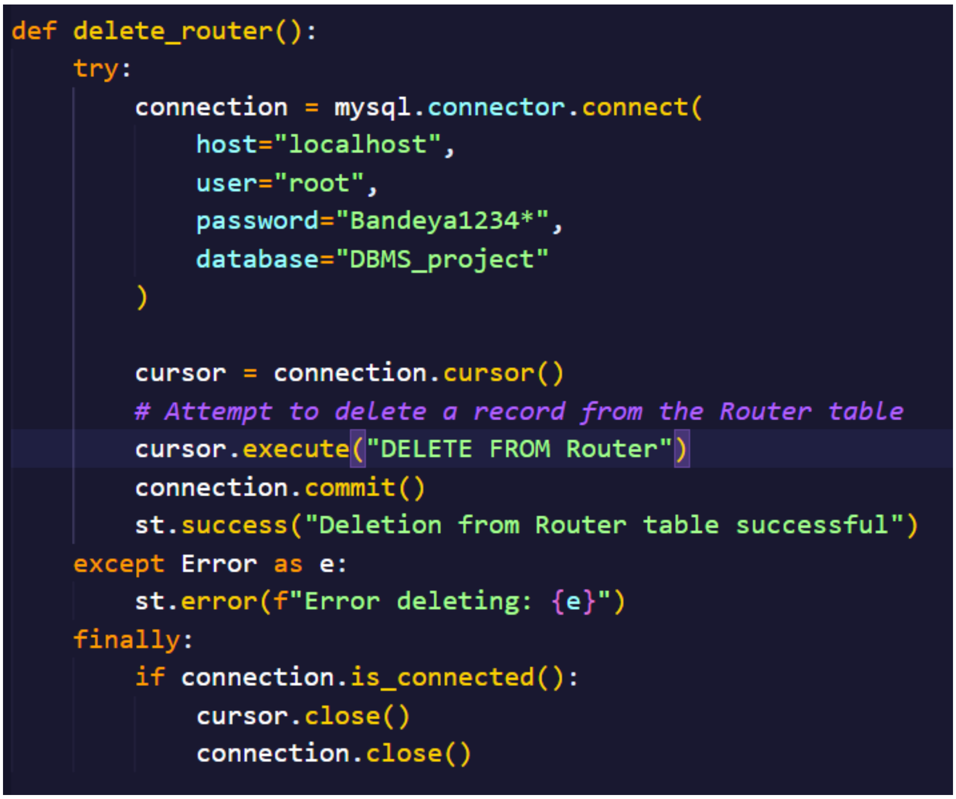
Choose an Option

Delete Router records

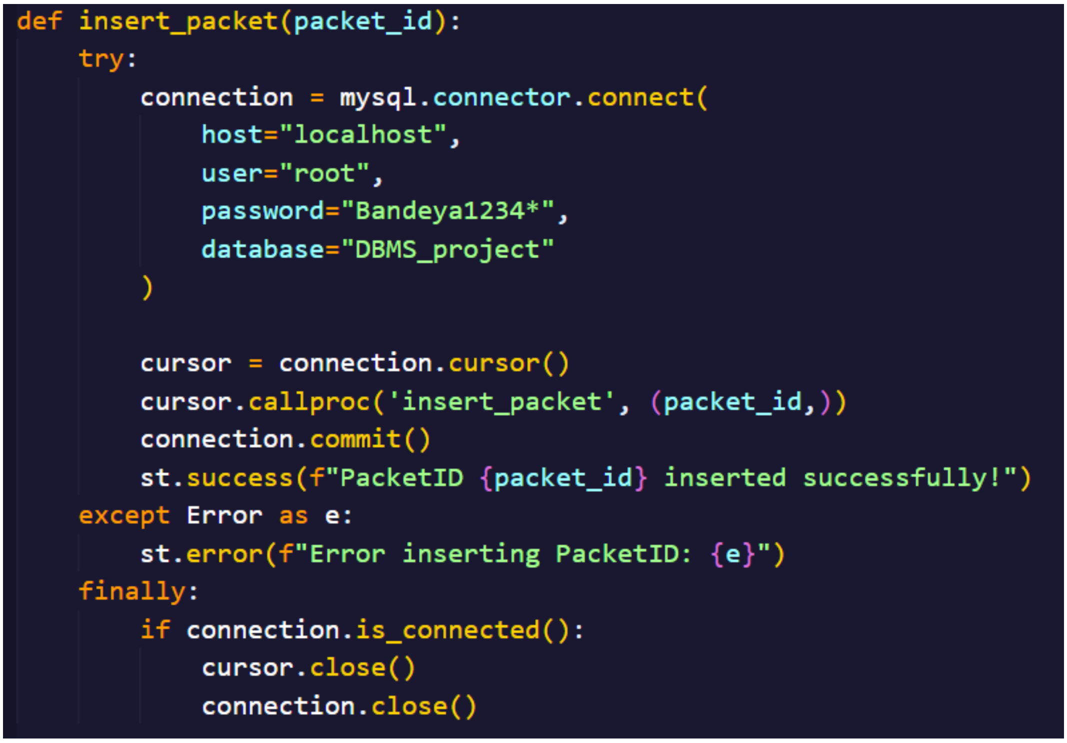
Error deleting: 1644 (45000): Deletion from the Router table is not allowed

The trigger to not allow deletion has been activated.

INVOKING OF PROCEDURE, TRIGGER:



```python
def delete_router():
    try:
        connection = mysql.connector.connect(
            host="localhost",
            user="root",
            password="Bandeya1234*",
            database="DBMS_project"
        )

        cursor = connection.cursor()
        # Attempt to delete a record from the Router table
        cursor.execute("DELETE FROM Router")
        connection.commit()
        st.success("Deletion from Router table successful")
    except Error as e:
        st.error(f"Error deleting: {e}")
    finally:
        if connection.is_connected():
            cursor.close()
            connection.close()
```



```python
def insert_packet(packet_id):
    try:
        connection = mysql.connector.connect(
            host="localhost",
            user="root",
            password="Bandeya1234*",
            database="DBMS_project"
        )

        cursor = connection.cursor()
        cursor.callproc('insert_packet', (packet_id,))
        connection.commit()
        st.success(f"PacketID {packet_id} inserted successfully!")
    except Error as e:
        st.error(f"Error inserting PacketID: {e}")
    finally:
        if connection.is_connected():
            cursor.close()
            connection.close()
```