SQL SCHEMA:

Schema For Storing Logs:

```
create table LogRecords (
logtime datetime(3),
ip varbinary(16),
request varchar(30),
statusvalue smallint,
useragent varchar(500),
primary key(ip,logtime))
```

- For Storing IP in the database, I am using varbinary(16). It stores binary String of the IP address. Varbinary(16) can store at maximum 128 bit binary string which is required for a IPv6 Address. For IPv4 varbinary(4) is sufficient. To handle both the cases I am using varbinary(16). Conversion from IP address to Binary String is done using the function 'INET6_ATON' and for back conversion to IP Address 'INET6_NTOA' is used in the queries.

Schema for Storing IP's that Matched the Condition:

```
create table IPLog (
ip varbinary(16),
reason varchar(35),
primary key(ip))
```

SQL QUERIES:

(1) Write MySQL query to find IPs that mode more than a certain number of requests for a given time period.

Ex: Write SQL to find IPs that made more than 100 requests starting from 2017-01-01.13:00:00 to 2017-01-01.14:00:00.

QUERY:

```
select inet6_ntoa(ip) as IPAddress
from logrecords
where logtime between '2017-01-01.13:00:00' and '2017-01-01.14:00:00'
group by ip
having count(*) >= 100;
```

(2) Write MySQL query to find requests made by a given IP.

QUERY:

Given IP: '192.168.11.231'

```
select inet6_ntoa(ip) as IPAddress, logtime, request, statusvalue, useragent
from logrecords where inet6_ntoa(ip) = '192.168.11.231';
```