MySQL 数据库日志审计实验

一【实验目标】

- 熟练管理和使用 MySQL 二进制日志
- 熟练使用日志文件恢复数据

二【实验环境】

- Windows 10
- MySQL 5.5

三【实验原理】

my.ini 配置信息的 log-bin 没有指定文件扩展名，这是因为即使你指定上扩展名它也不使用。当 mysql 创建二进制日志文件时，首先创建一个以“mysql_log_bin”为名称，以“.index”为后缀的文件；再创建一个以“mysql_log_bin”为名称，以“.000001”为后缀的文件。当 mysql 服务重新启动一次以“.000001”为后缀的文件会增加一个，并且后缀名加 1 递增；如果日志长度超过了 max_binlog_size 的上限(默认是 1G)也会创建一个新的日志文件；使用 flushlogs(mysql 命令符)或者执行 mysqladmin - u - pflush-logs(Windows 命令提示符)也会创建一个新的日志文件。

MySQL 的二进制日志文件是 MySQL 安全系统里的非常重要的文件，虽然打开日志，所有非 SELECT 的操作都会记录下来，但这在某些场合显得很冗余，比如还原数据库，或者导入数据等，日志文件会一条不漏的记录下所有的命令，这会使日志文件迅速变大。但正是因为这样，让数据库的安全性变得更加可靠。下面将通过日志文件恢复误操作，找回丢失的数据。

四【实验步骤】

1、输入密码【Admin123456】，登录系统。如图 1 所示。

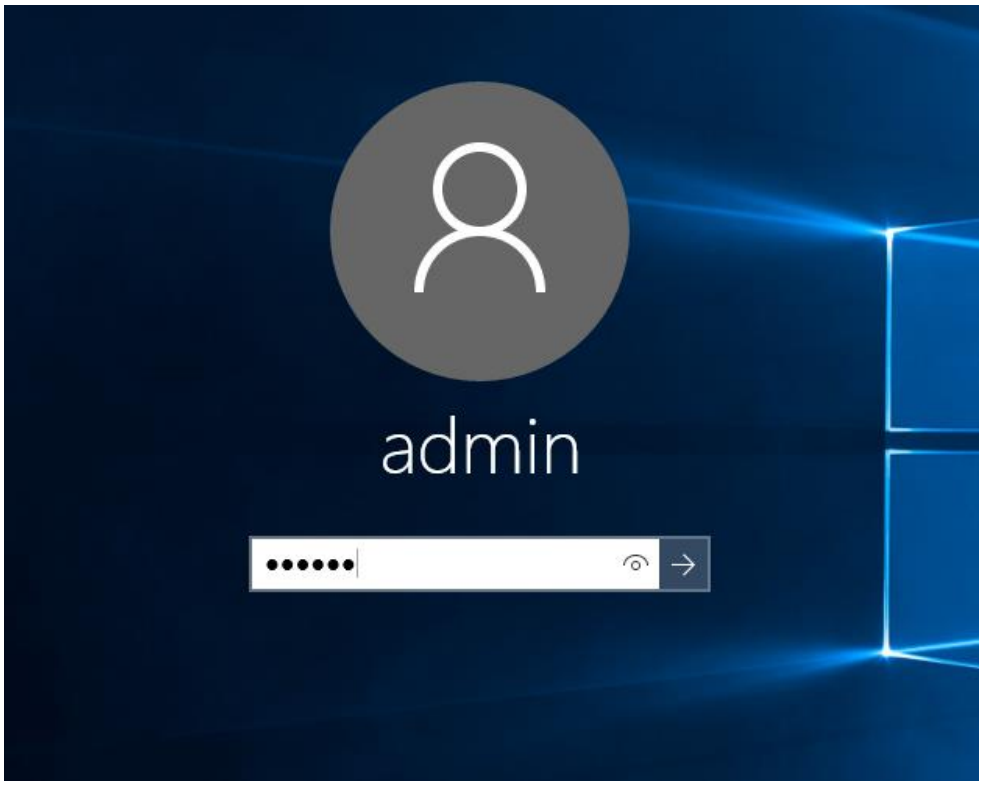

图 1

2、打开 MySQL 安装目录 C:\Tools\mysql\data。如图 2 所示。

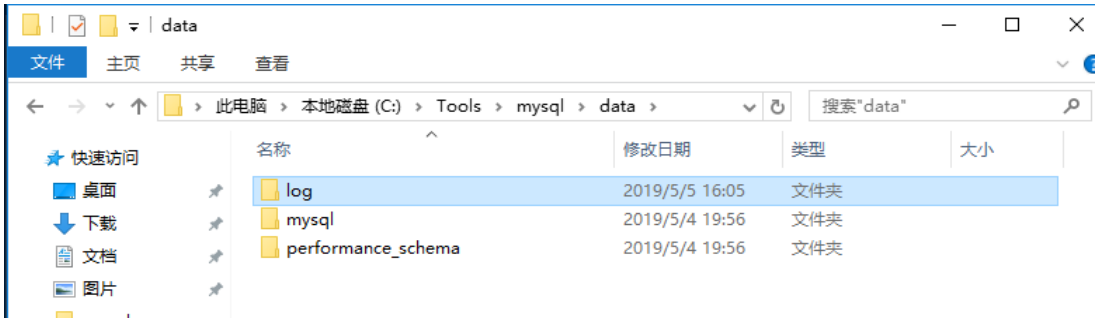

图 2

3、复制当前路径，如图 3 所示。

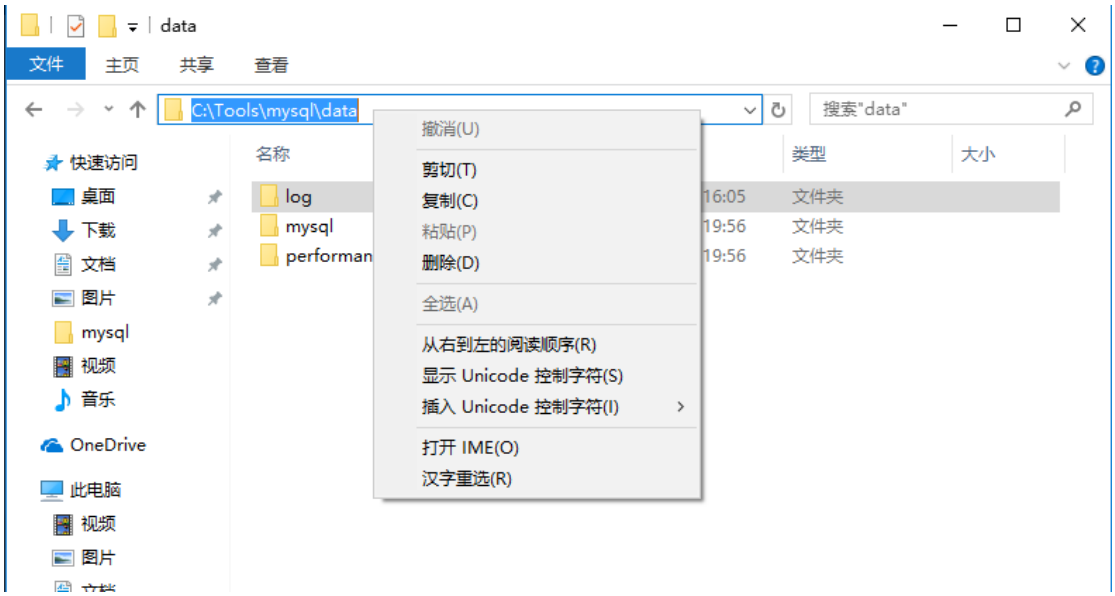

图 3

4、找到 MySQL 配置文件 my.ini。如图 4 所示。

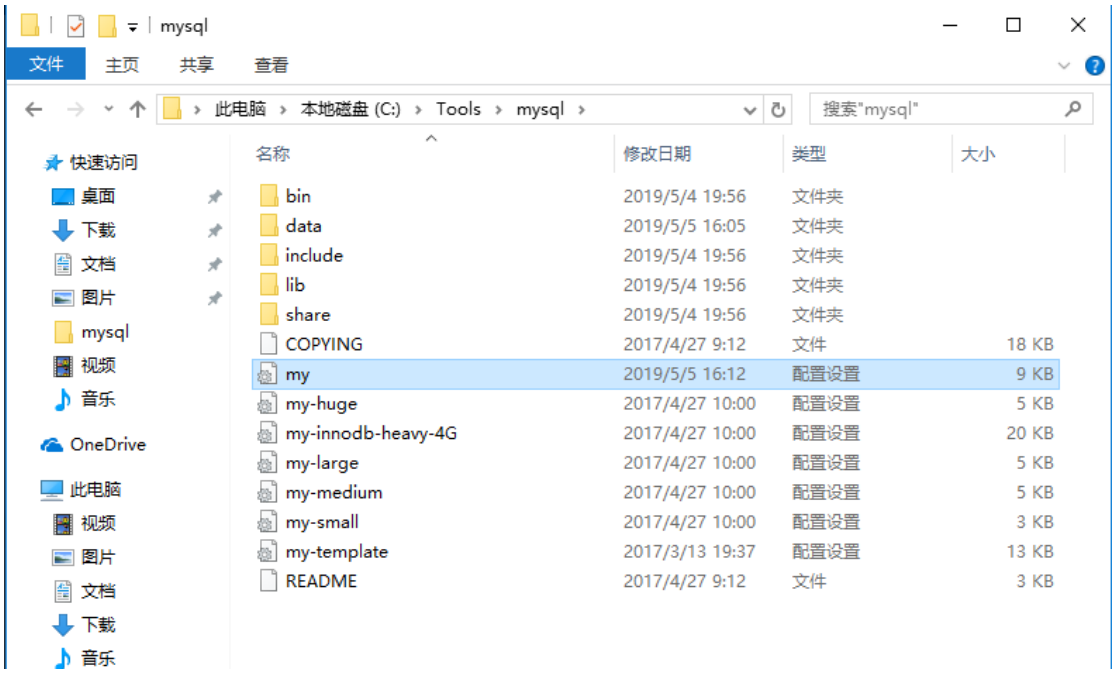

图 4

5、打开配置文件，在文件末尾添加内容

log-error=”C:/Tools/mysql/data/mysql_log_err.log”

log=”C:/Tools/mysql/data/mysql_log.log”

#log-update=”C:/Tools/mysql/data/mysql_log_update.txt”

log-bin=”C:/Tools/mysql/data/mysql_log_bin.bin”

long_query_time=1

log-slow-queries=” C:/Tools/mysql/data/mysql_log_slow.log”

如图 5 所示。

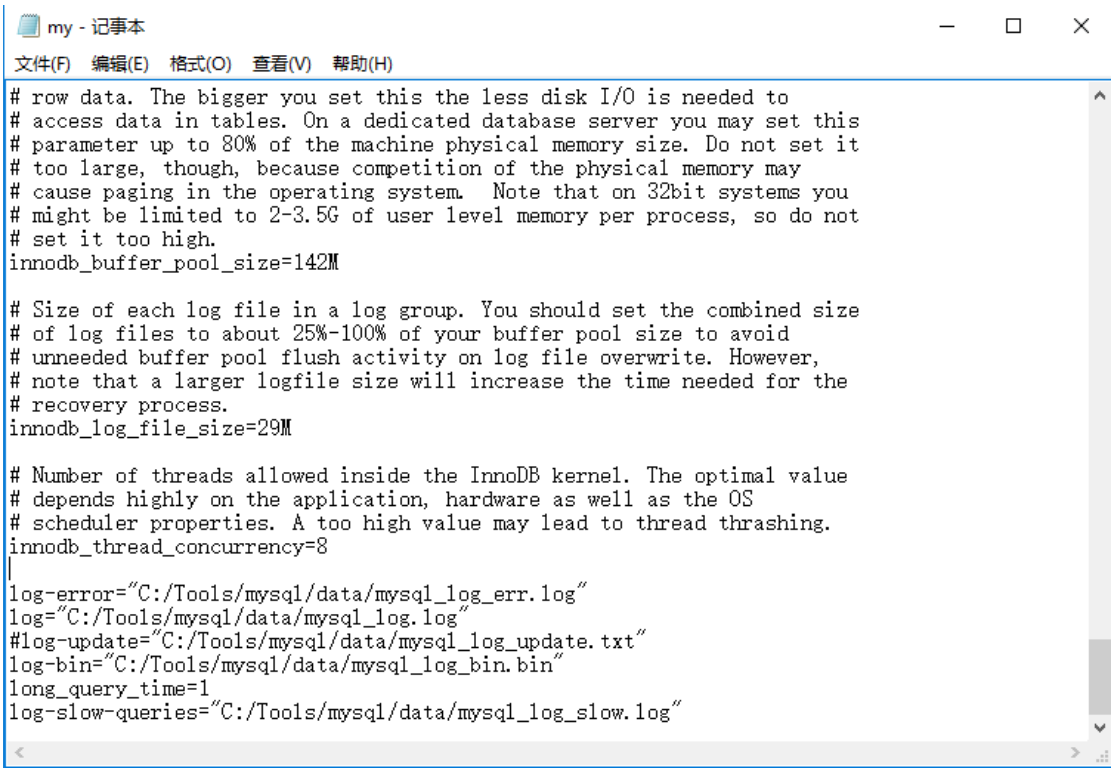

图 5

6、重启 MySQL 服务。如图 6 所示。

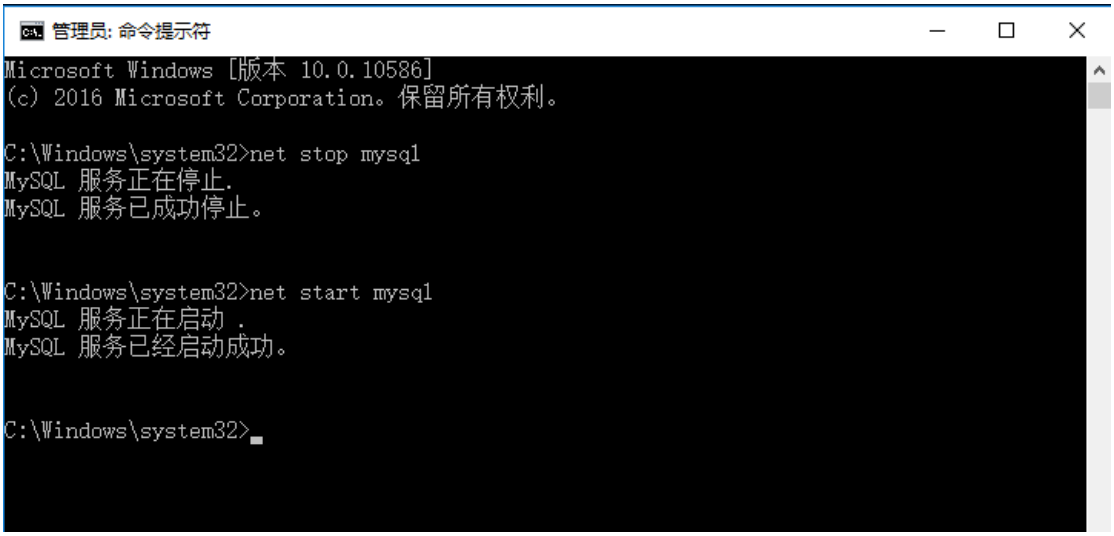

图 6

7、输入命令 show variables like ‘log_%’ ;,查看 MySQL 日志的关闭与开启。如图 7 所示。

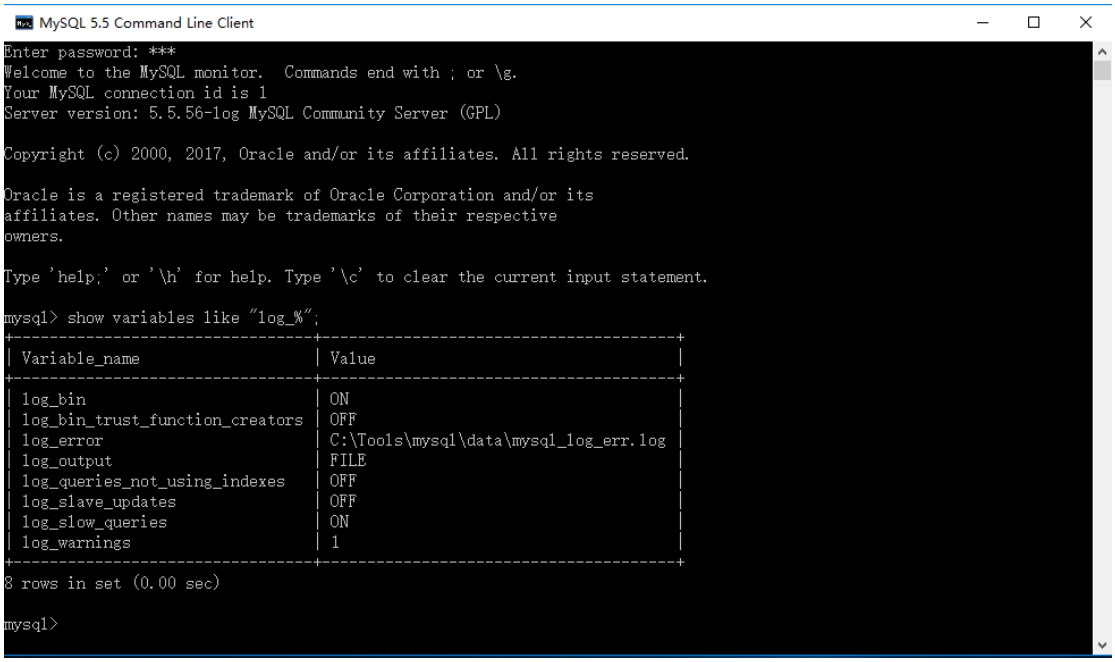

图 7

8、输入命令：mysqlbinlog C:\Tools\mysql\data\mysql_log_bin.000001 查看日志。如图 8 所示。

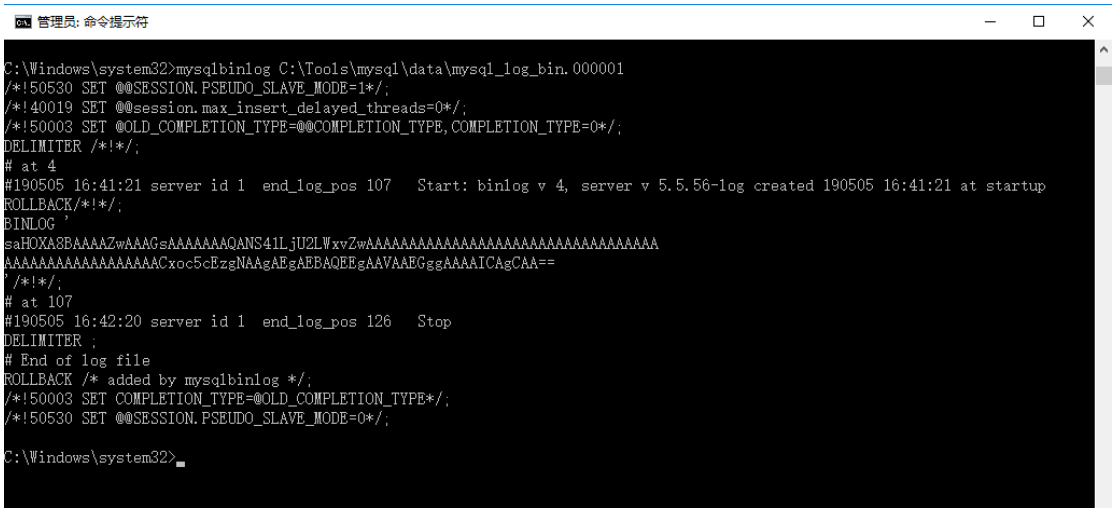

图 8

9、输入命令：show master logs;查看二进制日志数目。如图 9 所示。

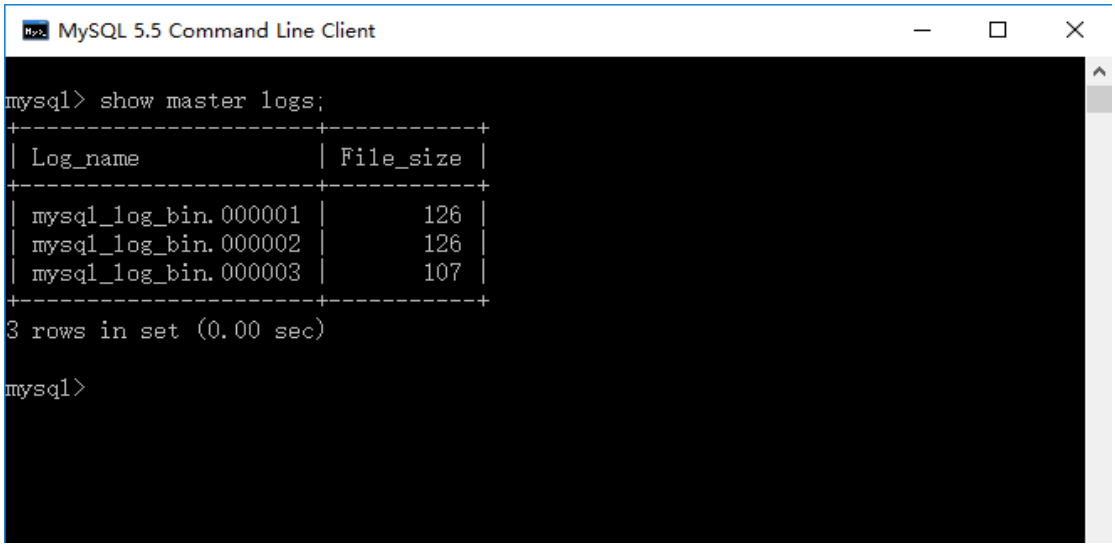

图 9

10、输入命令：show master status;查看当前二进制日志。如图 10 所示。

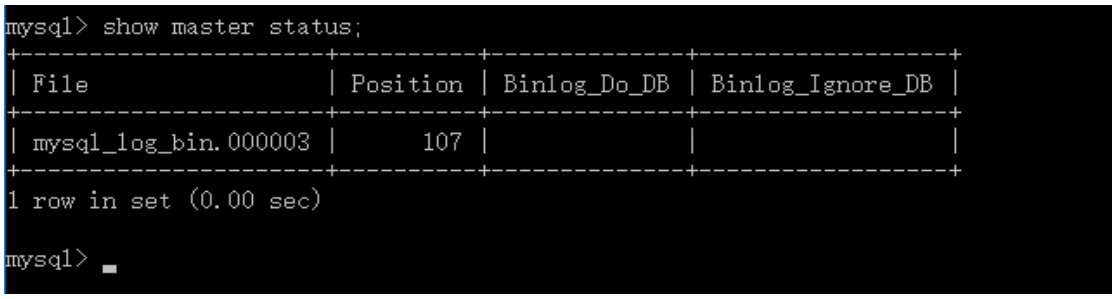

图 10

11、输入命令：mysqlbinlog C:\Tools\mysql\data\mysql_log_bin.000001 >aabb.sql 将二进制的日志文件转换成.sql 的文件，并输入命令 dir 查看。如图 11 所示。

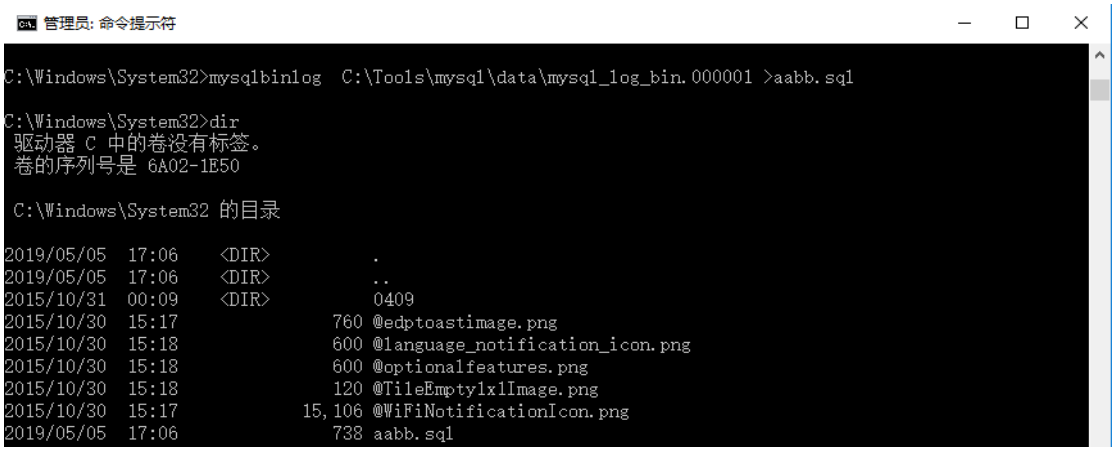

图 11

12、打开数据库，执行“use test;”切换到 test 数据库下，执行“show tables;”命令查看该数据库中的表，执行命令“create table student(id int, name char(50), age int);”创建新表 student。如图 12 所示。

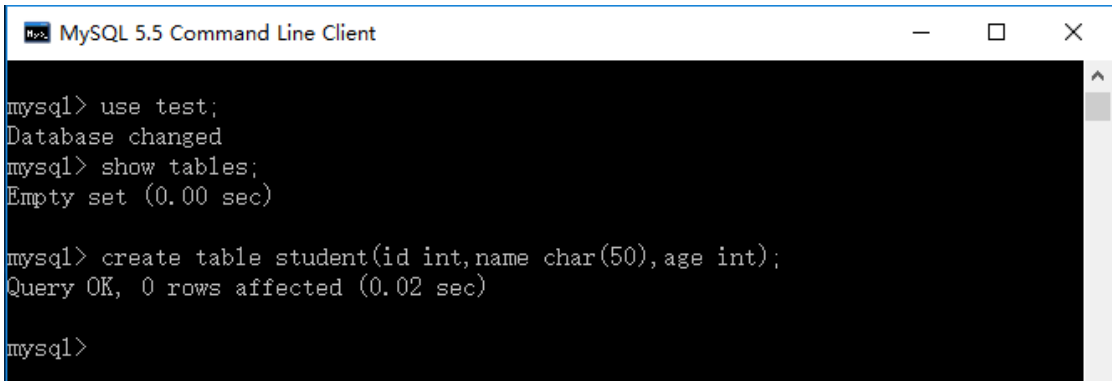

图 12

13、向 student 表中插入数据，并查询 student 表，如图 13 所示。

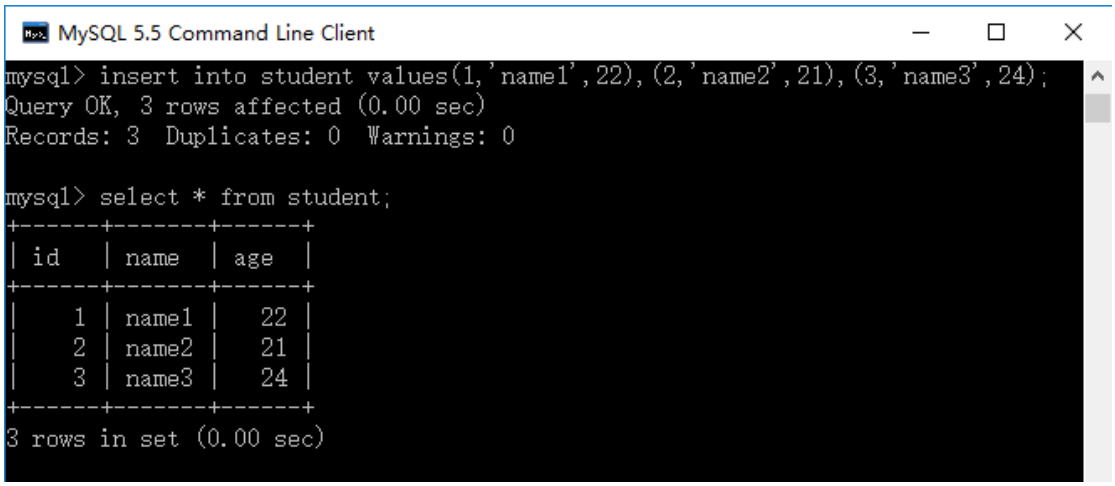

图 13

14、删除 student 表中数据，删除表，如图 14 所示。

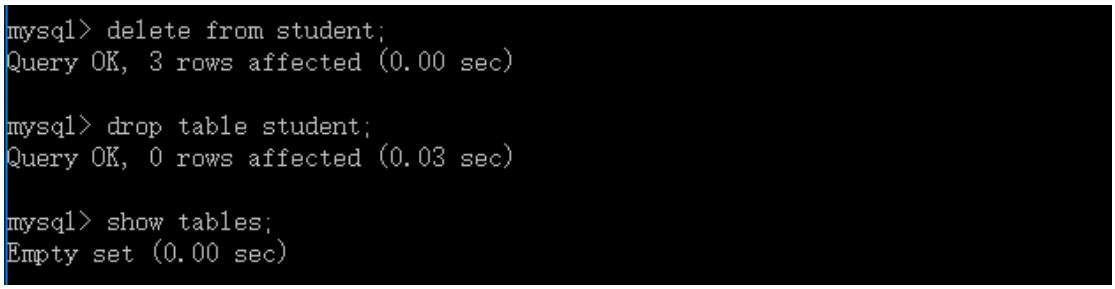

图 14

15、查看二进制日志，后缀编号同第九步一致。如图 15 和图 16 所示。

图 15

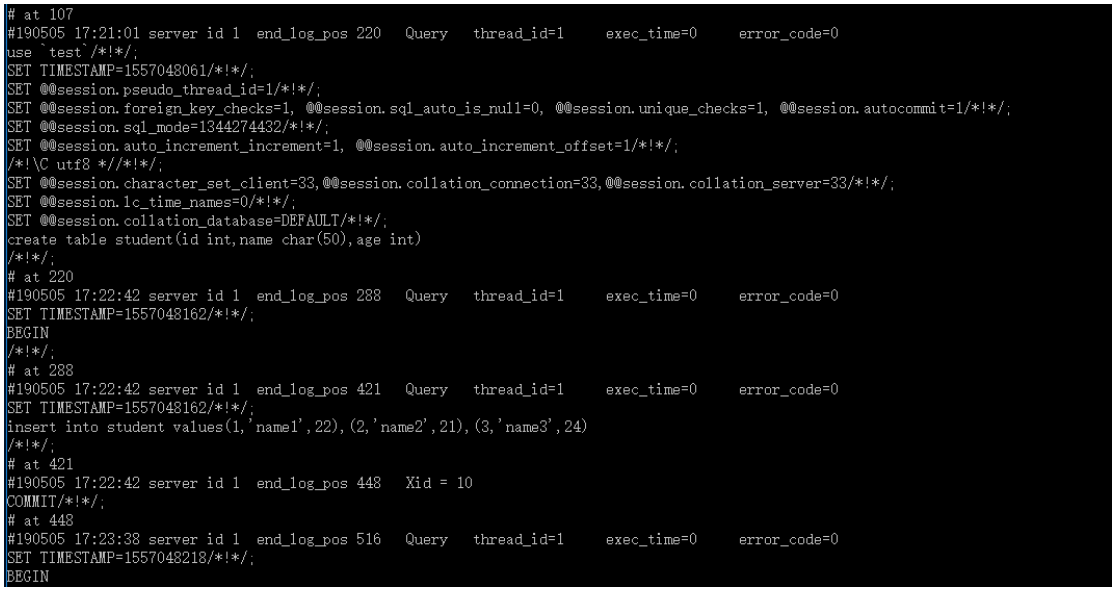

图 16

16、截取日志的第 107 行至 448 行，其中 107 为第九步中 position 的值 448 为删除操作开始前的值，存入 107448.sql 文件，如图 17 所示。

图 17

17、把提取出来的日志文件段导入到数据库中，如图 18 所示。

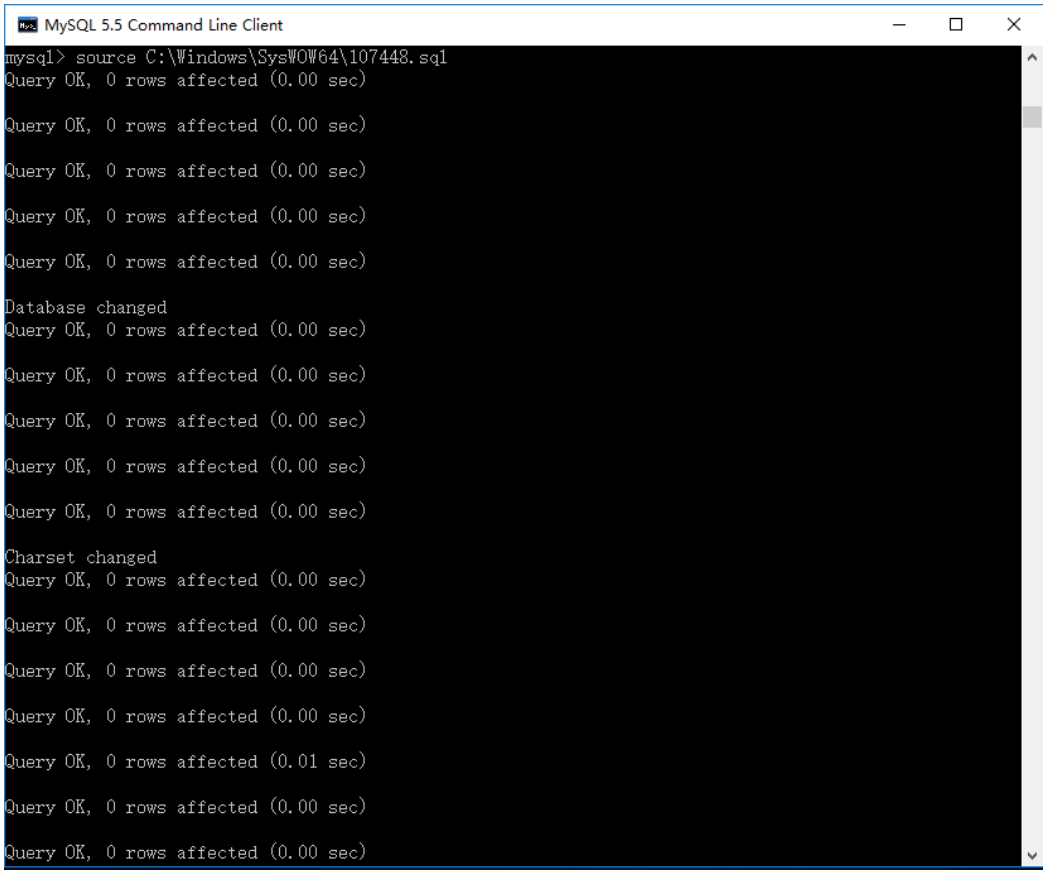

图 18

18、查看恢复的结果，如图 19 所示。

```
mysql> show tables;
+----------------+
| Tables_in_test |
+----------------+
| student        |
+----------------+
1 row in set (0.00 sec)

mysql> select * from student;
+------+-------+------+
| id   | name  | age  |
+------+-------+------+
|    1 | name1 |   22 |
|    2 | name2 |   21 |
|    3 | name3 |   24 |
+------+-------+------+
3 rows in set (0.00 sec)
```

图 19

五【实验思考】

- 通过日志恢复数据与通过备份恢复数据各有何优劣？