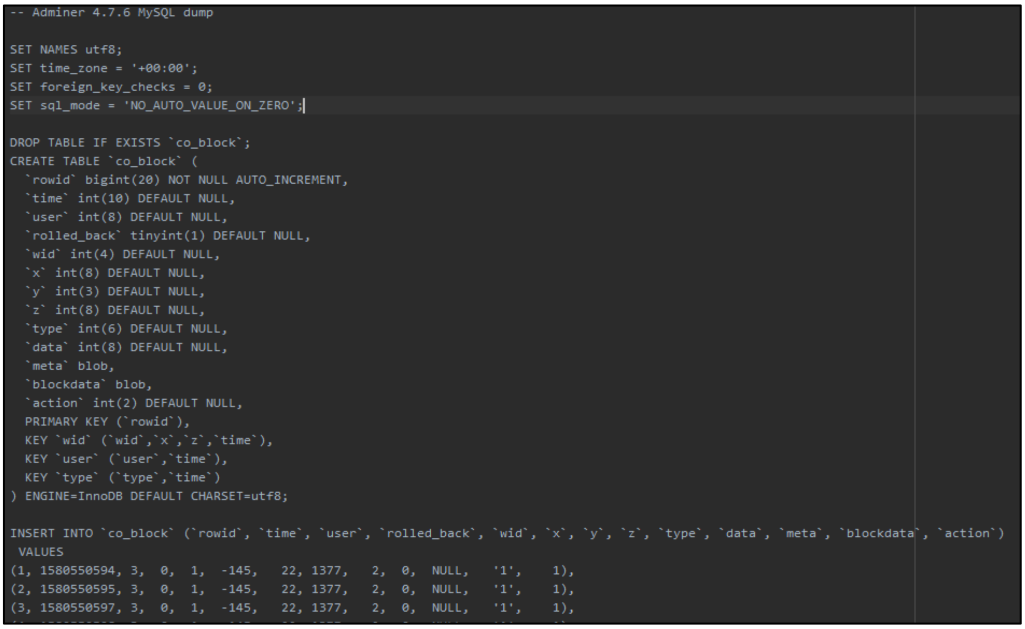
Forensics : Block2

Description : Billy runs a Minecraft server. He wants to know which block was rolled back. Can you help him?

Attachment : co_block.sql.gz

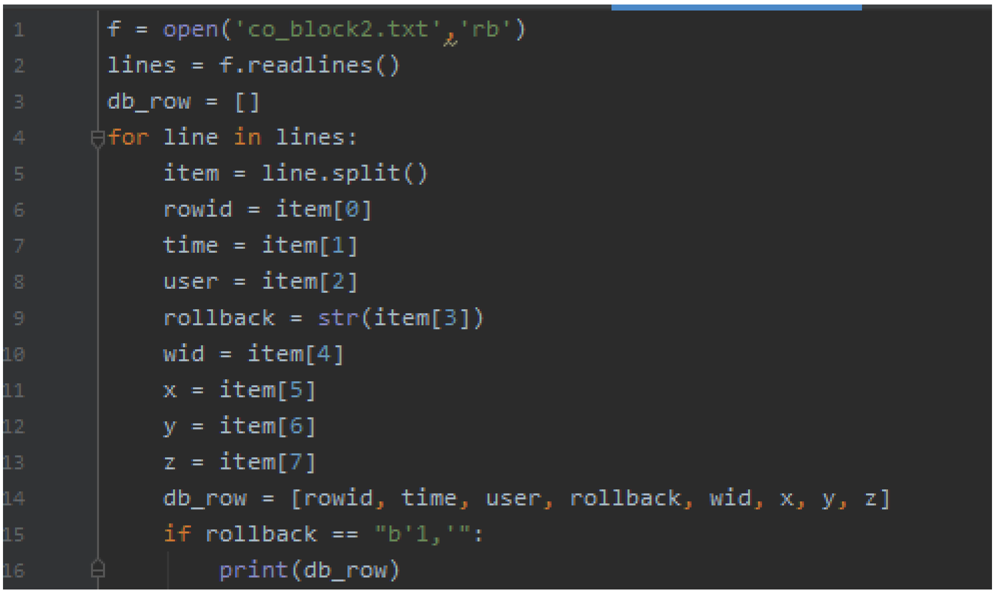
Solutions :

1. Unzip Attachment file.
2. Open this co_block.sql file in PyCharm.

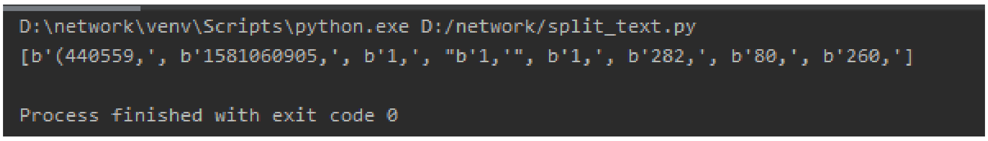


```
-- Adminer 4.7.6 MySQL dump

SET NAMES utf8;
SET time_zone = '+00:00';
SET foreign_key_checks = 0;
SET sql_mode = 'NO_AUTO_VALUE_ON_ZERO';

DROP TABLE IF EXISTS `co_block`;
CREATE TABLE `co_block` (
  `rowid` bigint(20) NOT NULL AUTO_INCREMENT,
  `time` int(10) DEFAULT NULL,
  `user` int(8) DEFAULT NULL,
  `rolled_back` tinyint(1) DEFAULT NULL,
  `wid` int(4) DEFAULT NULL,
  `x` int(8) DEFAULT NULL,
  `y` int(3) DEFAULT NULL,
  `z` int(8) DEFAULT NULL,
  `type` int(6) DEFAULT NULL,
  `data` int(8) DEFAULT NULL,
  `meta` blob,
  `blockdata` blob,
  `action` int(2) DEFAULT NULL,
  PRIMARY KEY (`rowid`),
  KEY `wid` (`wid`,`x`,`z`,`time`),
  KEY `user` (`user`,`time`),
  KEY `type` (`type`,`time`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;

INSERT INTO `co_block` (`rowid`, `time`, `user`, `rolled_back`, `wid`, `x`, `y`, `z`, `type`, `data`, `meta`, `blockdata`, `action`)
 VALUES
(1, 1580550594, 3,  0,  1,  -145,   22, 1377,   2,  0,  NULL,   '1',    1),
(2, 1580550595, 3,  0,  1,  -145,   22, 1377,   2,  0,  NULL,   '1',    1),
(3, 1580550597, 3,  0,  1,  -145,   22, 1377,   2,  0,  NULL,   '1',    1),
```

3. Check point columns (rolled_back).
4. It can be confirmed that the Rolled_back column is set to 1 when rolled back.
5. Search for rows with the rolled_back column set to 1.



```python
f = open('co_block2.txt','rb')
lines = f.readlines()
db_row = []
for line in lines:
    item = line.split()
    rowid = item[0]
    time = item[1]
    user = item[2]
    rollback = str(item[3])
    wid = item[4]
    x = item[5]
    y = item[6]
    z = item[7]
    db_row = [rowid, time, user, rollback, wid, x, y, z]
    if rollback == "b'1,'":
        print(db_row)
```



```
D:\network\venv\Scripts\python.exe D:/network/split_text.py
[b'(440559,', b'1581060905,', b'1,', "b'1,'", b'1,', b'282,', b'80,', b'260,']

Process finished with exit code 0
```

6. Only one row is found.

7. Flag is 1581060905

   Flag : auctf{1581060905}