

DIGITAL FORENSICS FOR MYSQL

-LOG 분석

김태훈 (Go by Francesco, kkomak.wordpress.com)



분석 대상

- MYSQL DBMS 로그인 이력
- DDL 사용 이력
- DML 사용 이력

분석 대상 Artifacts

분류	항목	관련 Artifacts
로그인 이력	홈페이지 등 웹 어플리케이션을 통한 로그인	General Query Log
	DBMS 관리 툴을 통한 DBA 접근	General Query Log
정보 조회	정보 조회 등 수행 이력	General Query Log
정보 변경	데이터 변경/삭제 수행 이력	General Query Log Binary Log
데이터베이스 변경	테이블 생성/삭제	General Query Log Binary Log

General Query Log



The server writes information to this log **when** clients **connect** or **disconnect**, and it logs each **SQL statement** received from **clients**.



The general query log can be very useful **when** you suspect an error in a client and want to know exactly **what** the client sent to **mysqld**.



The general query log is a general record of **what mysqld is doing**.

General Query Log



- 로그 포맷: READABLE 가능한 TEXT 로그 포맷
- 로그 활성화: 기본 설정은 비활성화 되어 있음
- 로그 위치: 로그 설정 정보 참조

General Query Log

GENERAL Query LOG 디폴트 설정은 OFF 임.

```
mysql> show variables like '%general%';
+-----+-----+
| Variable_name | Value
+-----+-----+
| general_log   | OFF
| general_log_file | /var/lib/mysql/4322502b4a80.log |
+-----+-----+
2 rows in set (0.00 sec)

mysql> set global general_log=on;
Query OK, 0 rows affected (0.01 sec)

mysql> show variables like '%general%';
+-----+-----+
| Variable_name | Value
+-----+-----+
| general_log   | ON
| general_log_file | /var/lib/mysql/4322502b4a80.log |
+-----+-----+
2 rows in set (0.00 sec)
```

1. docker exec -it 43 /bin/bash (ssh)

```
root@4322502b4a80:/var/lib/mysql#
root@4322502b4a80:/var/lib/mysql# pwd
/var/lib/mysql
root@4322502b4a80:/var/lib/mysql#
root@4322502b4a80:/var/lib/mysql# ls -alc *.log
-rw-r---- 1 mysql mysql 27084 Dec  2 09:48 4322502b4a80.log
root@4322502b4a80:/var/lib/mysql# █
```

General Query Log

:: General Query Log Format ::

Time (GMT)

Id

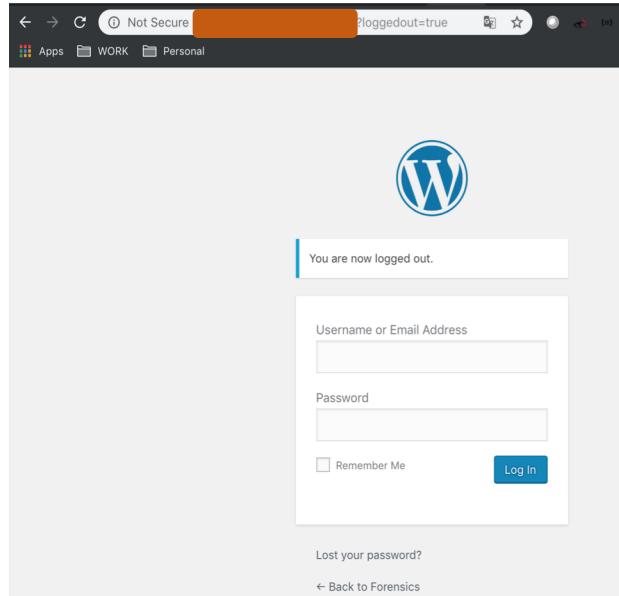
Command

Argument

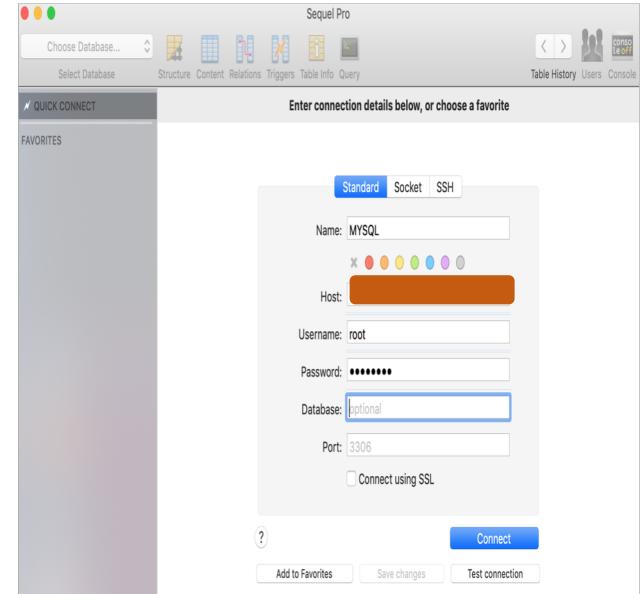
2018-12-02T09:45:01.859679Z 5 Connect wordpress@172.18.0.3 on using TCP/IP

General Query Log

:: WORDPRESS ::



:: DBMS 관리 툴 ::



General Query Log

WEB Application 로그인 인증 관련 로그

Time	Id	Command	Argument	ETC
2018-12-02T09:45:01.859679Z	5	Connect	wordpress@172.18.0.3 on using TCP/IP	웹 서버와 MYSQL 서버 간의 연결 정보
2018-12-02T09:45:01.869155Z	5	Query	SELECT * FROM ab_users WHERE user_login = 'francesco'	사용자 조회 Query

```
root@4322502b4a80:/var/lib/mysql# cat 4322502b4a80.log
Time                                         Id   Command          Argument
2018-12-02T09:45:01.859679Z                  5    Connect         wordpress@172.18.0.3 on using TCP/IP
2018-12-02T09:45:01.859918Z                  5    Query          SET NAMES utf8mb4
2018-12-02T09:45:01.860286Z                  5    Query          SET NAMES 'utf8mb4' COLLATE 'utf8mb4_unicode_520_ci'
2018-12-02T09:45:01.860387Z                  5    Query          SELECT @@SESSION.sql_mode
2018-12-02T09:45:01.860532Z                  5    Query          SET SESSION sql_mode='NO_ZERO_IN_DATE,ERROR_FOR_DIVISION_BY_ZERO,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION'
2018-12-02T09:45:01.860639Z                  5    Init DB        mydbname
2018-12-02T09:45:01.869155Z                  5    Query          SELECT option_name, option_value FROM ab_options WHERE autoload = 'yes'
2018-12-02T09:45:02.185056Z                  5    Query          SELECT * FROM ab_users WHERE user_login = 'francesco'
2018-12-02T09:45:02.186523Z                  5    Query          SELECT user_id, meta_key, meta_value FROM ab_usermeta WHERE user_id IN (1) ORDER BY umeta_id ASC
```

General Query Log

DBMS 관리 툴 및 로컬 CLI 접속

The image displays two main sections: the MySQL General Query Log and a MySQL terminal session.

MySQL General Query Log: This section shows a list of log entries from December 2018. The log entries are timestamped and show various MySQL commands. A yellow callout box highlights several entries, including:

- 19 Connect root@127.0.0.1 on using TCP/IP
- 19 Query SHOW VARIABLES
- 19 Query SELECT @@global.max_allowed_packet
- 19 Query SHOW DATABASES
- 20 Connect root@127.0.0.1 on using TCP/IP
- 20 Query SHOW VARIABLES
- 20 Query SELECT @@global.max_allowed_packet
- 19 Query USE `mydbname`
- 19 Query SHOW VARIABLES LIKE 'character_set_database'
- 19 Query SHOW /*!50002 FULL*/ TABLES

A blue callout box highlights the first two log entries:

- 18 Connect root@localhost on using Socket
- 18 Query select @@version_comment limit 1

MySQL Terminal Session: This section shows a MySQL command-line interface session. It includes:

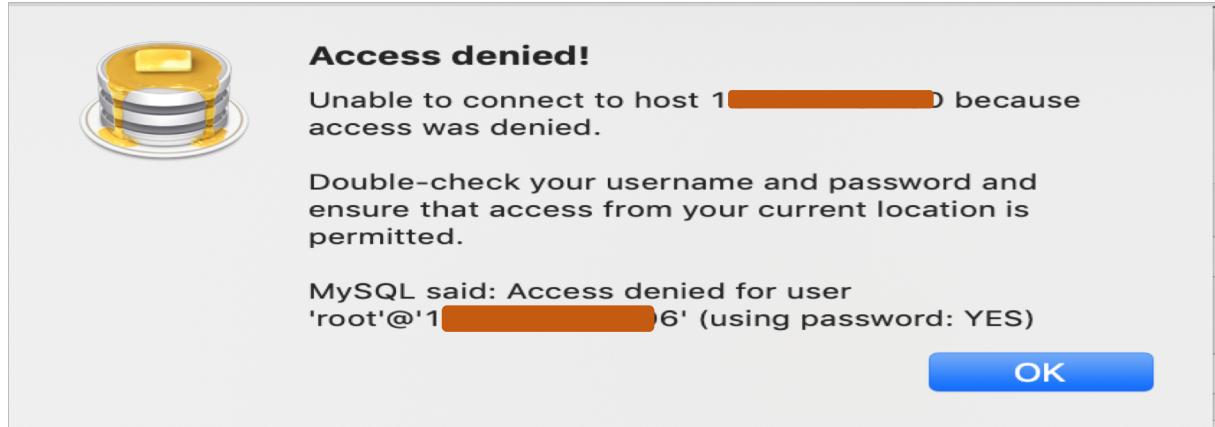
- Connection details: Host [REDACTED], Username: root, Password: [REDACTED], Database: [optional], Port: 3306, Connect using SSL.
- Welcome message: Welcome to the MySQL monitor. Commands end with ; or \g.
- Server version: 5.7.24 MySQL Community Server (GPL)
- Copyright notice: Copyright (c) 2000, 2018, Oracle and/or its affiliates. All rights reserved.
- Trademark notice: MySQL is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective
- Help message: Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
- Show databases command output:

```
+-----+  
| Database |  
+-----+  
| information_schema |  
| mydbname |  
| mysql |  
| performance_schema |  
| sys |  
+-----+
```

5 rows in set (0.01 sec)
- Exit command: mysql> exit
Bye

General Query Log

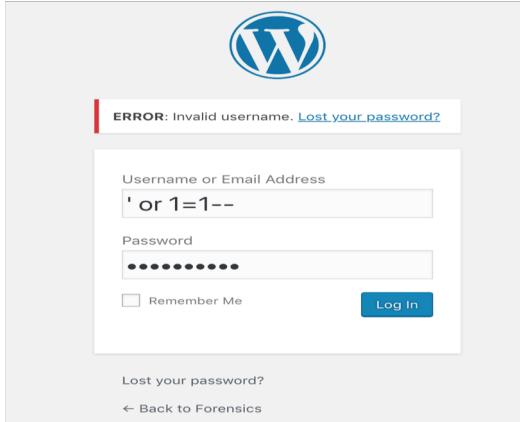
DBMS 관리 툴을 이용한 로그인 실패



```
2018-12-02T10:38:16.488801Z      21 Connect  root@1[REDACTED] on using TCP/IP
2018-12-02T10:38:16.488848Z      21 Connect  Access denied for user 'root'@'[REDACTED]' (using password: YES)
root@0432502b4a80:/var/lib/mysql#
```

General Query Log

웹 어플리케이션 취약점 공격 관련 로그 :: SQL Injection



```
2018-12-02T10:40:33.029204Z 22 Connect wordpress@172.18.0.3 on  using TCP/IP
2018-12-02T10:40:33.029366Z 22 Query SET NAMES utf8mb4
2018-12-02T10:40:33.029541Z 22 Query SET NAMES 'utf8mb4' COLLATE 'utf8mb4_unicode_520_ci'
2018-12-02T10:40:33.029626Z 22 Query SELECT @@SESSION.sql_mode
2018-12-02T10:40:33.029756Z 22 Query SET SESSION sql_mode='NO_ZERO_IN_DATE,ERROR_FOR_DIVISION_BY_ZERO,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION'
2018-12-02T10:40:33.029842Z 22 Init DB mydbname
2018-12-02T10:40:33.030308Z 22 Query SELECT option_name, option_value FROM ab_options WHERE autoload = 'yes'
2018-12-02T10:40:33.030842Z 22 Query SELECT option_value FROM ab_options WHERE option_name = 'WPLANG' LIMIT 1
2018-12-02T10:40:33.035339Z 22 Query SHOW FULL COLUMNS FROM `ab_options`
2018-12-02T10:40:33.035796Z 22 Query UPDATE `ab_options` SET `option_value` = '1543747233.0351989269256591796875' WHERE `option_name` = '_transient_doing_cron'
2018-12-02T10:40:34.040588Z 22 Query SELECT option_value FROM ab_options WHERE option_name = 'theme_switched' LIMIT 1
2018-12-02T10:40:34.041157Z 22 Query SELECT * FROM ab_users WHERE user_login = '\\\' or 1=1--
2018-12-02T10:40:34.041495Z 22 Query SELECT * FROM ab_users WHERE user_login = '\\\' or 1=1--
2018-12-02T10:40:34.042207Z 22 Query SELECT option_value FROM ab_options WHERE option_name = 'can_compress_scripts' LIMIT 1
2018-12-02T10:40:34.042739Z 22 Query SELECT * FROM ab_posts WHERE ID = 3 LIMIT 1
2018-12-02T10:40:34.043190Z 22 Quit
```

General Query Log

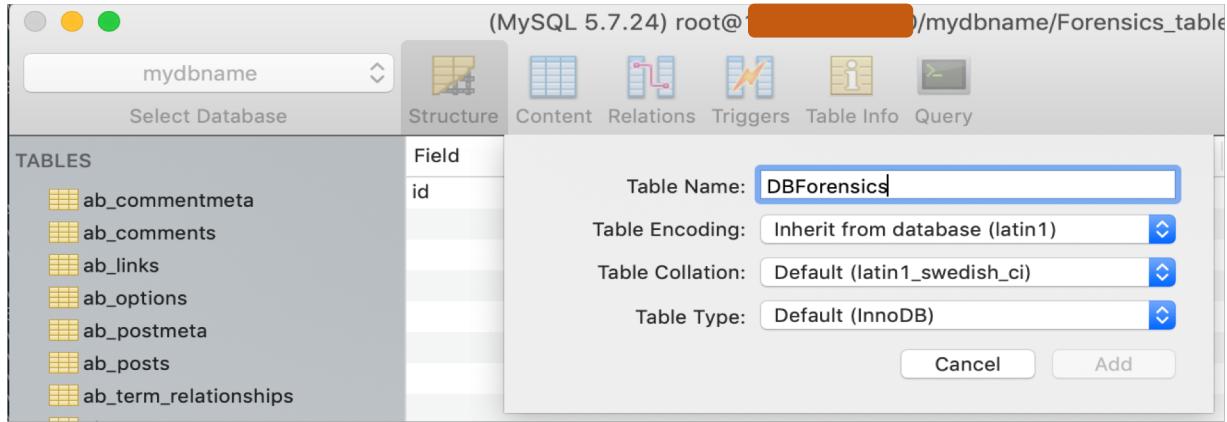
DBMS 관리 툴을 이용한 데이터 수정

The screenshot shows the MySQL Workbench interface. The title bar indicates the connection is to MySQL 5.7.24 root@127.0.0.1 mydbname/ab_users. The left sidebar lists tables: ab_commentmeta, ab_comments, ab_links, ab_options, ab_postmeta, ab_posts, ab_term_relationships, ab_term_taxonomy, ab_termmeta, ab_terms, ab_usermeta, and ab_users. The 'ab_users' table is selected and displayed in the main pane. A search bar at the top right shows 'Search: ID'. The table has columns: ID, user_login, user_pass, user_nicename, and user_email. One row is visible: ID 1, user_login francesco, user_pass \$P\$, user_nicename francesco, user_email ki...o2@gmail.com. Below the table, a log of recent queries is shown:

Time	Thread ID	Query Type	Query
2018-12-03T11:36:52.777460Z	24	Query	SELECT Engine, Support FROM `information_schema`.`engines` WHERE SUPPORT IN ('DEFAULT', 'YES')
2018-12-03T11:36:55.783004Z	24	Query	SHOW COLUMNS FROM `ab_users`
2018-12-03T11:37:04.551520Z	24	Query	UPDATE `ab_users` SET `user_email` = 'ki...o2@gmail.com' WHERE `ID` = '1'
2018-12-03T11:37:04.561236Z	24	Query	SELECT * FROM `ab_users` LIMIT 0,1000

General Query Log

DBMS 관리 툴을 이용한 테이블 생성



```
2018-12-03T12:48:39.712490Z 24 Query SET NAMES 'utf8'  
2018-12-03T12:48:39.718362Z 24 Query CREATE TABLE `DBForensics` (id INT(11) UNSIGNED NOT NULL PRIMARY KEY AUTO_INCREMENT)  
2018-12-03T12:48:39.748770Z 24 Query SHOW TABLE STATUS LIKE 'DBForensics'  
2018-12-03T12:48:39.758631Z 24 Query SHOW CREATE TABLE `DBForensics`  
2018-12-03T12:48:39.764485Z 24 Query SET NAMES 'latin1'  
2018-12-03T12:48:39.811387Z 24 Query SHOW INDEX FROM `DBForensics`  
2018-12-03T12:48:39.822729Z 24 Query SELECT COUNT(1) FROM `DBForensics`  
2018-12-03T12:48:39.860547Z 25 Query SHOW FULL COLUMNS FROM `ab_commentmeta` FROM `mydbname`
```

General Query Log

DBMS 관리 툴을 이용한 테이블 삭제



2018-12-03T12:53:19.703876Z	24	Query	DROP TABLE `DBForensics`
2018-12-03T12:53:19.724565Z	25	Query	SHOW FULL COLUMNS FROM `ab_commentmeta` FROM `mydbname`
2018-12-03T12:53:19.735672Z	25	Query	SHOW FULL COLUMNS FROM `ab_comments` FROM `mydbname`
2018-12-03T12:53:19.746602Z	25	Query	SHOW FULL COLUMNS FROM `ab_links` FROM `mydbname`

Binary Log



This log consists of one or more files that record statement that modifies the database.



It contains a record of statements such as DELETE, INSERT, REPLACE, CREATE TABLE, DROP TABLE, GRANT, and REVOKE



Binary log contents are written as SQL statements encoded in binary format

Binary Log

BINARY LOG 디폴트 설정은 OFF 임.

```
⚡ root@ip-172-31-10-7 ~francesco/WORK/Docker/web_mysql_compose> cat docker-compose.yml
version: '2'

services:
  wordpress:
    image: wordpress:latest
    links:
      - database:mysqlDb
    environment:
      - WORDPRESS_DB_USER=wordpress
      - WORDPRESS_DB_NAME=mydbname
      - WORDPRESS_TABLE_PREFIX=ab_
      - WORDPRESS_DB_PASSWORD=dbforensics
      - WORDPRESS_DB_HOST=mysqlDb
      - MYSQL_PORT_3306_TCP=3306
    restart: unless-stopped
    ports:
      - "80:80"
    working_dir: /var/www/html
    volumes:
      - ./wordpress:/var/www/html/
  database:
    image: mysql:5.7
    environment:
      - MYSQL_ROOT_PASSWORD=*****
      - MYSQL_DATABASE=mydbname
      - MYSQL_USER=wordpress
      - MYSQL_PASSWORD=dbforensics
    command: ["mysqld", "--log-bin=mysql-bin", "--server-id=1"]
    restart: unless-stopped
    ports:
      - "3306:3306"
⚡ root@ip-172-31-10-7 ~francesco/WORK/Docker/web_mysql_compose>
```

```
mysql> show variables like '%log_bin%';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| log_bin       | ON    |
| log_bin_basename | /var/lib/mysql/mysql-bin |
| log_bin_index | /var/lib/mysql/mysql-bin.index |
| log_bin_trust_function_creators | OFF   |
| log_bin_use_v1_row_events | OFF   |
| sql_log_bin   | ON    |
+-----+-----+
6 rows in set (0.01 sec)

mysql>
```

Binary Log

WORDPRESS에서 게시물 INSERT한 내역

Posts [Add New](#)

All (2) | Published (2)

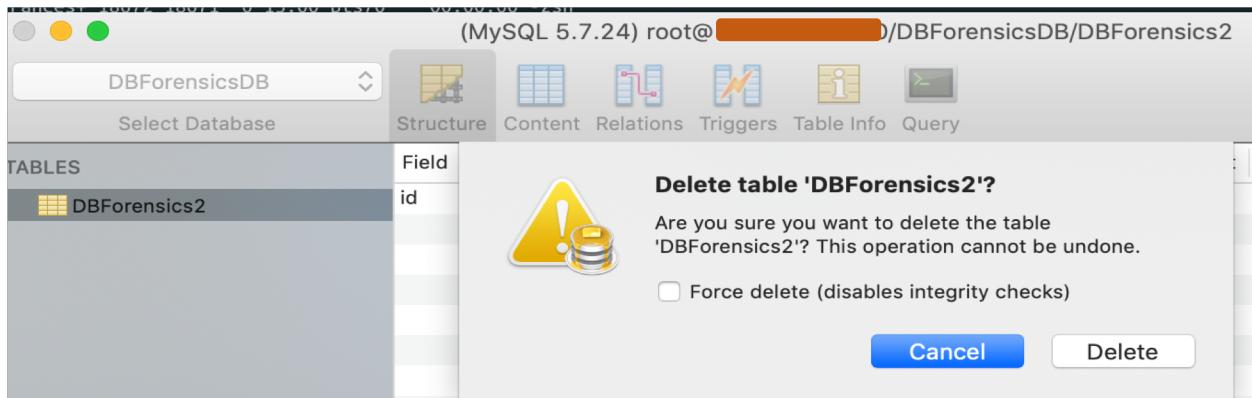
Bulk Actions All dates All Categories

<input type="checkbox"/> Title	Author	Categories
<input type="checkbox"/> TEST FOR FORENSICS Edit Quick Edit Trash View	francesco	Uncategorized

```
deWyc X - 2 mysql mysql 12288 Dec 3 15:50 sys
root@c443237d7f9e:/var/lib/mysql# mysqlbinlog -vv mysql-bin.000003 | grep FORENSICS
### @6='TEST FOR FORENSICS' /* BLOB/TEXT meta=2 nullable=0 is_null=0 */
### @6='TEST FOR FORENSICS' /* BLOB/TEXT meta=2 nullable=0 is_null=0 */
### @5='TEST FOR FORENSICS' /* LONGBLOB/LONGTEXT meta=4 nullable=0 is_null=0 */
### @6='TEST FOR FORENSICS' /* BLOB/TEXT meta=2 nullable=0 is_null=0 */
### @5='TEST FOR FORENSICS' /* LONGBLOB/LONGTEXT meta=4 nullable=0 is_null=0 */
### @6='TEST FOR FORENSICS' /* BLOB/TEXT meta=2 nullable=0 is_null=0 */
### @5='TEST FOR FORENSICS' /* LONGBLOB/LONGTEXT meta=4 nullable=0 is_null=0 */
### @6='TEST FOR FORENSICS' /* BLOB/TEXT meta=2 nullable=0 is_null=0 */
### @5='TEST FOR FORENSICS' /* LONGBLOB/LONGTEXT meta=4 nullable=0 is_null=0 */
### @6='TEST FOR FORENSICS' /* BLOB/TEXT meta=2 nullable=0 is_null=0 */
root@c443237d7f9e:/var/lib/mysql# mysqlbinlog -vv mysql-bin.000002 | grep FORENSICS
root@c443237d7f9e:/var/lib/mysql# mysqlbinlog -vv mysql-bin.000001 | grep FORENSICS
root@c443237d7f9e:/var/lib/mysql#
```

Binary Log

DBMS 관리 툴에서 테이블 삭제



```
SET @SESSION.GTID_NEXT= 'ANONYMOUS'/* */;
# at 1499200
#181203 16:18:00 server id 1  end_log_pos 1499336 CRC32 0xeeedc43      Query    thread_id=59      exec_time=0      error_code=0
SET TIMESTAMP=1543853880/*!*/;
/*!|C latin1 *//*!*/;
SET @@session.character_set_client=8,@@session.collation_connection=8,@@session.collation_server=8/*!*/;
RENAME TABLE `DBForensics` TO `DBForensics2`
/*!*/;
# at 1499336
#181203 16:18:58 server id 1  end_log_pos 1499401 CRC32 0x30c15377      Anonymous_GTID  last_committed=264      sequence_number=265      rbr_only=no
SET @SESSION.GTID_NEXT= 'ANONYMOUS'/*!*/;
# at 1499401
#181203 16:18:58 server id 1  end_log_pos 1499544 CRC32 0xd115456      Query    thread_id=59      exec_time=0      error_code=0
SET TIMESTAMP=1543853938/*!*/;
DROP TABLE `DBForensics2` /* generated by server */
/*!*/;
```

Update Log



The update log is similar to the binary log, but it is stored in text format and does not contain as much information.