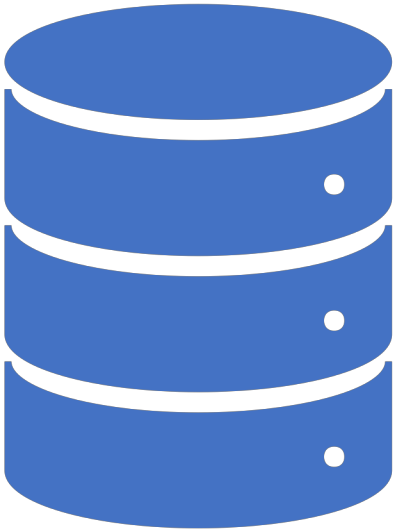
DIGITAL FORENSICS FOR MYSQL
-LOG 분석

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.

REFERENCE: https://dev.mysql.com/doc/refman/5.7/en/query-log.html

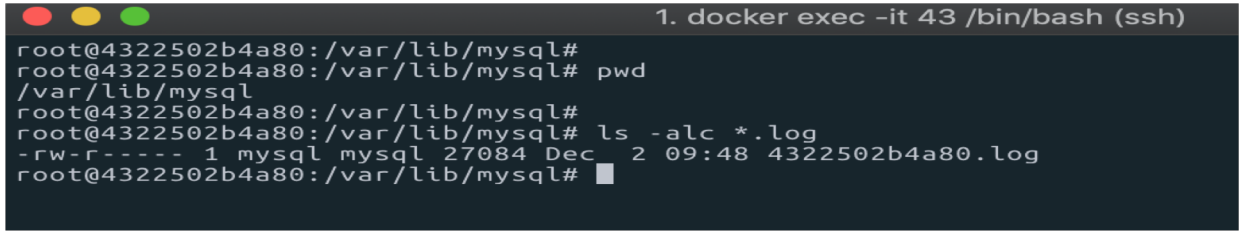
General Query Log

- 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)
```



General Query Log

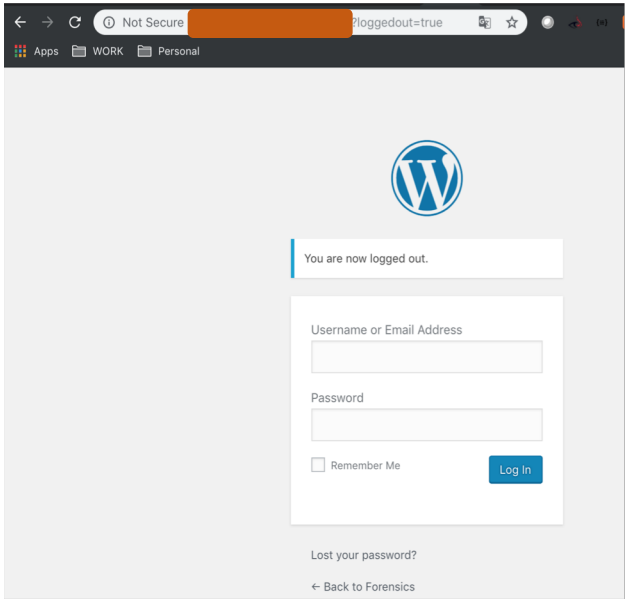
:: General Query Log Format ::

Time (GMT)	Id	Command	Argument

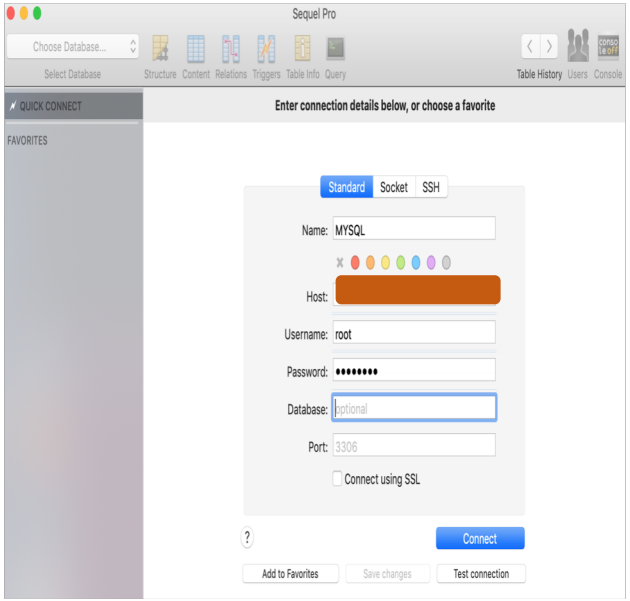
2018-12-02T09:45:01.859679Z 5 Connect wordpress@172.18.0.3 on using TCP/IP

General Query Log

:: WORDPRESS ::



:: DBMS 관리 툴 ::



General Query Log

WEB Application 로그인 인증 관련 로그

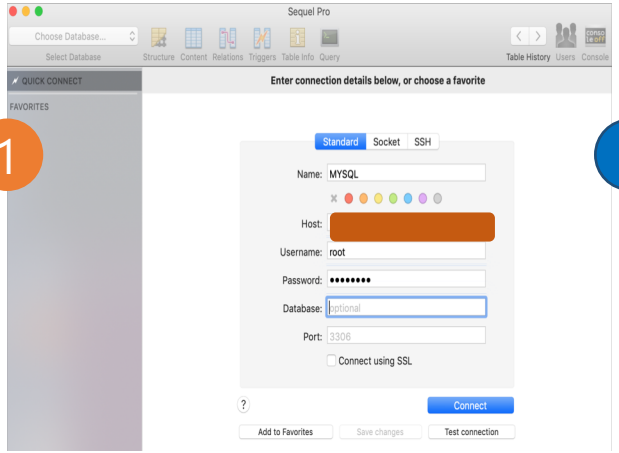
Time	Id	Command	Argument	ETC
2018-12-02T09:45:01.859679Z	5	Connect	wordpress@172.18.0.3 on using TCP/IP	웹 서버와 MYSQL 서버 간의 연결 정보
2018-12-02T09:45:01.869155Z	5	Query	SELECT * FROM ab_users WHERE user_login = 'francesco'	사용자 조회 Query

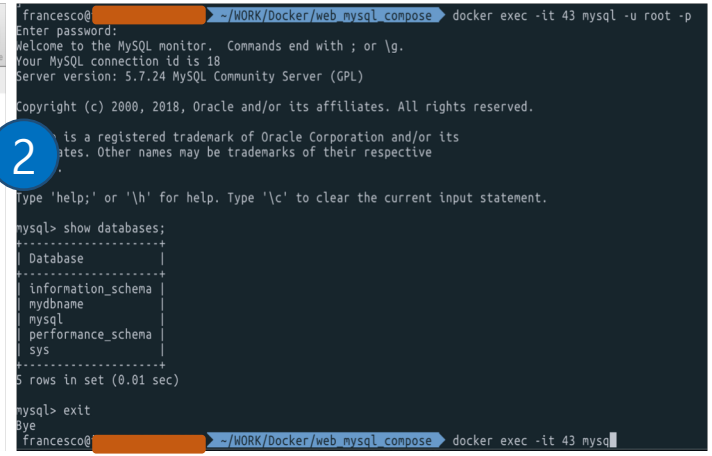
root@4322502b4a80:/var/lib/mysql# cat 4322502b4a80.log

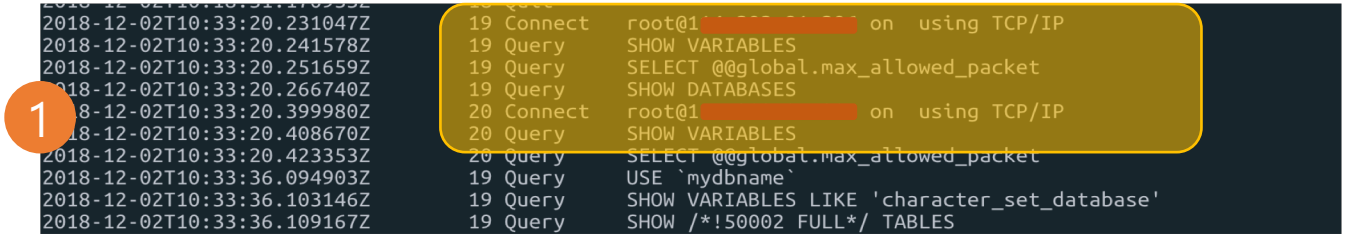
Time	Id	Command	Argument
2018-12-02T09:45:01.859679Z	**5**	**Connect**	**wordpress@172.18.0.3 on using TCP/IP**
2018-12-02T09:45:01.859918Z	5	Query	SET NAMES utf8mb4
2018-12-02T09:45:01.860286Z	5	Query	SET NAMES 'utf8mb4' COLLATE 'utf8mb4_unicode_520_ci'
2018-12-02T09:45:01.860387Z	5	Query	SELECT @@SESSION.sql_mode
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

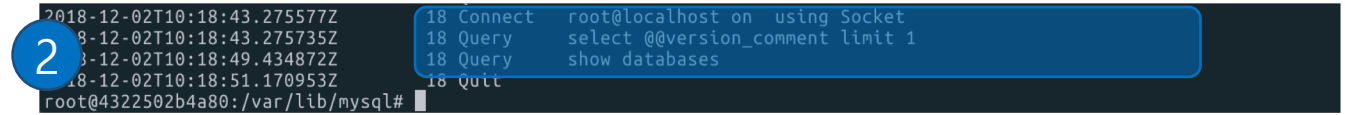
DBMS 관리 툴 및 로컬 CLI 접속

General Query Log



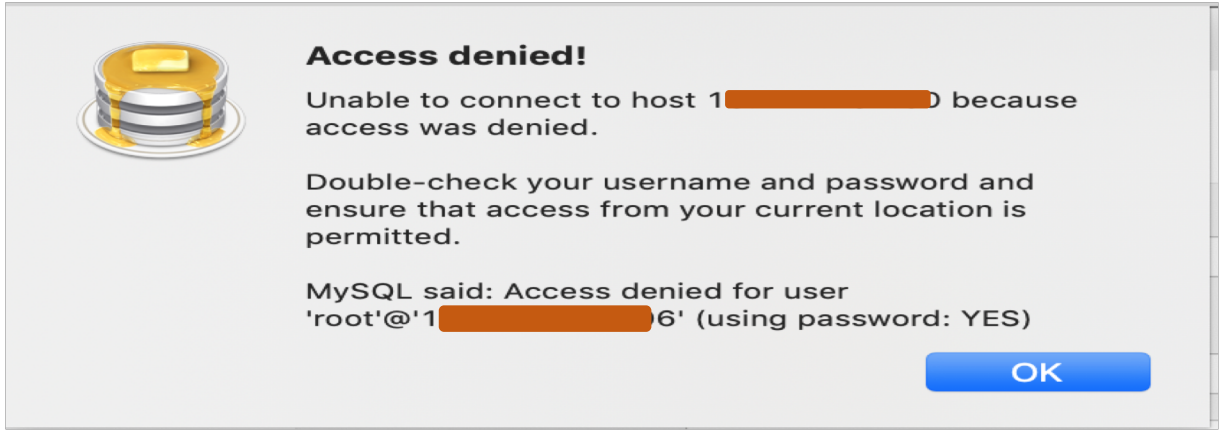






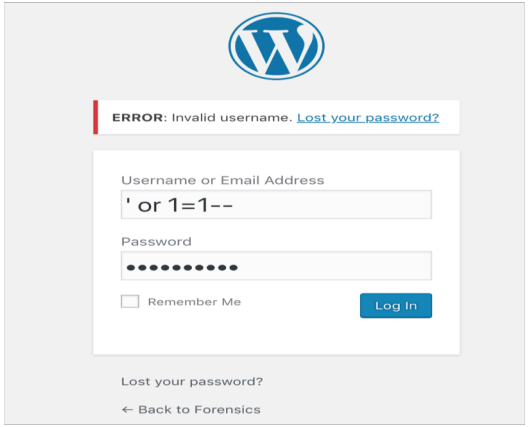
General Query Log

DBMS 관리 툴을 이용한 로그인 실패



웹 어플리케이션 취약점 공격 관련 로그 ::: SQL Injection

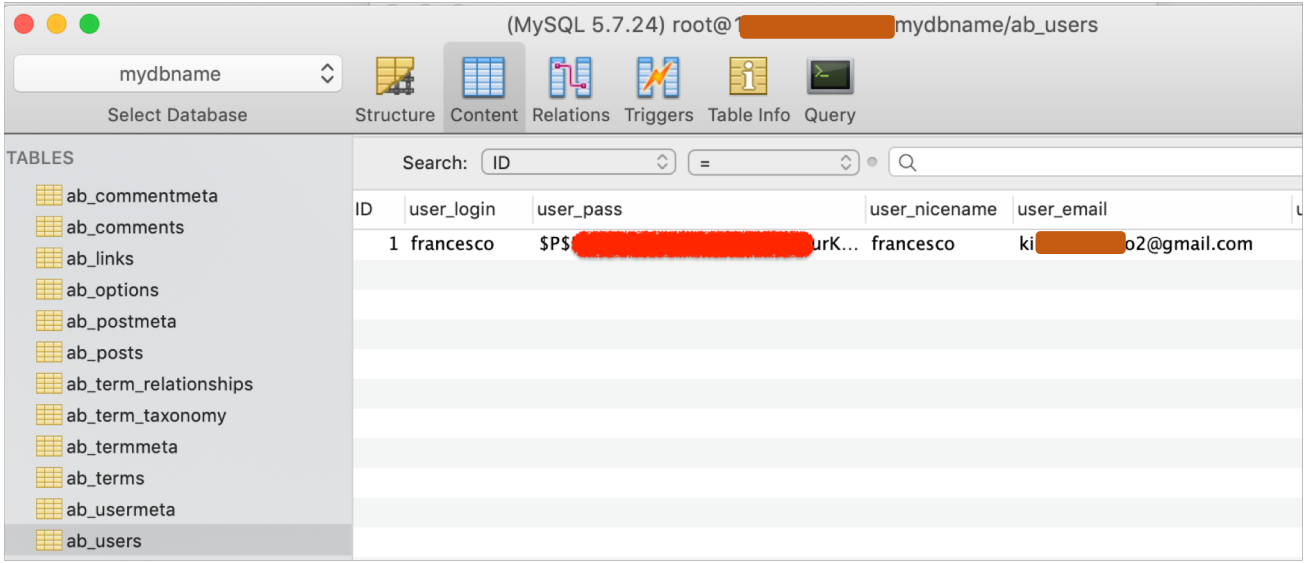
General Query Log




```
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'
2018-12-02T10:40:33.033084Z       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
```

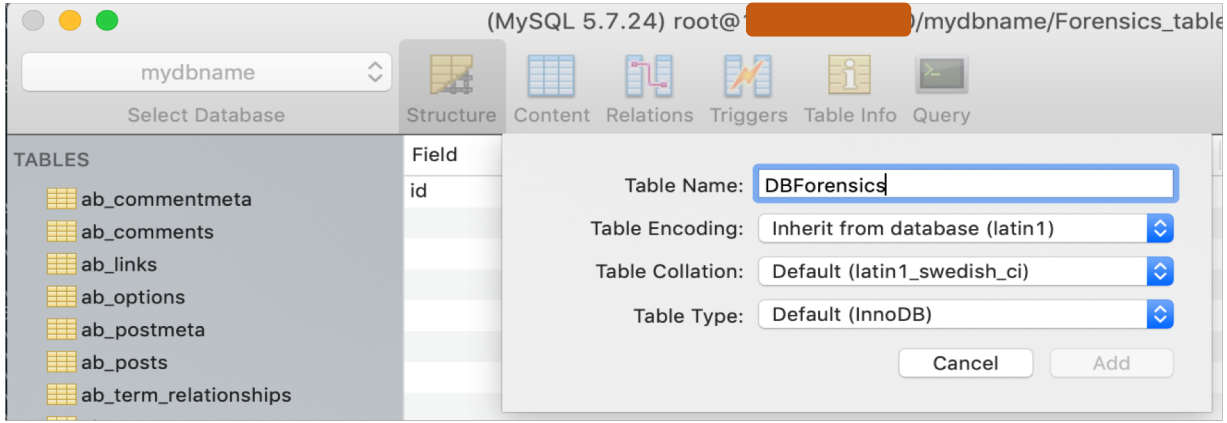
DBMS 관리 툴을 이용한 데이터 수정

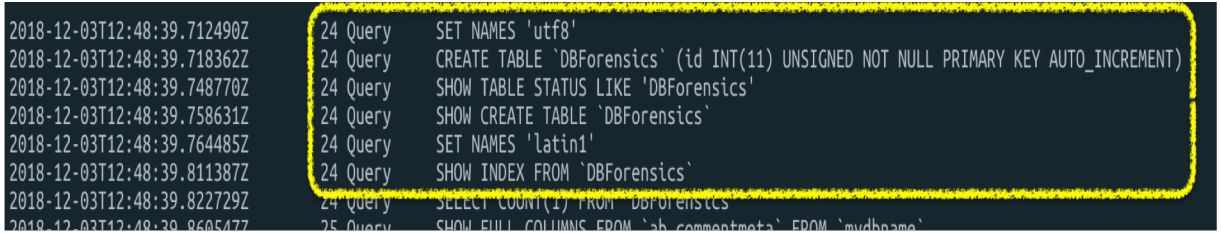
General Query Log



General Query Log

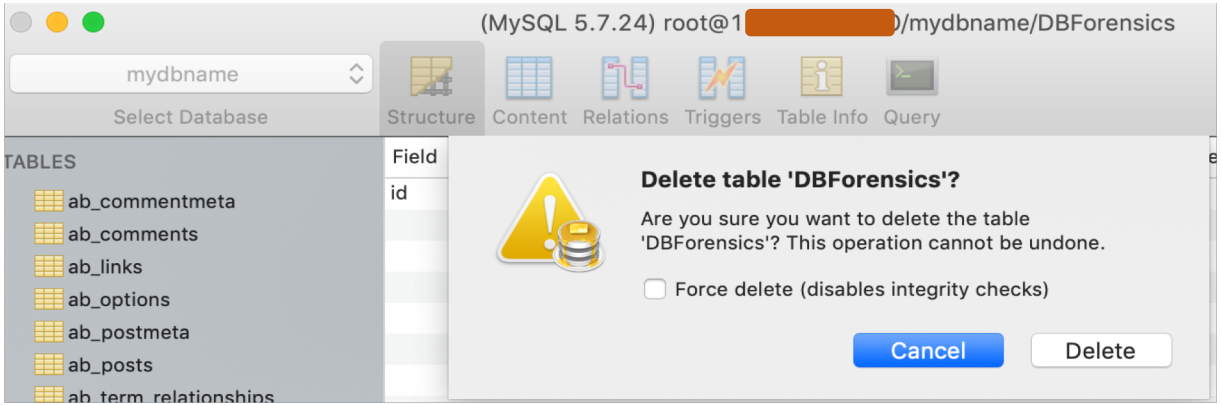
DBMS 관리 툴을 이용한 테이블 생성

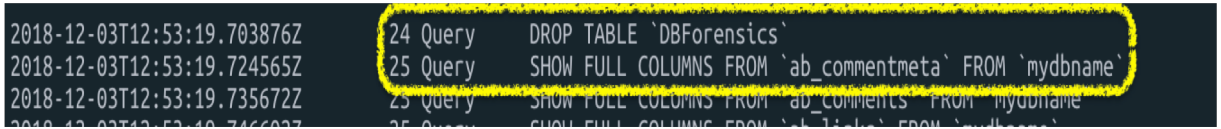




DBMS 관리 툴을 이용한 테이블 삭제

General Query Log





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 디폴트 설정은 OFF 임.

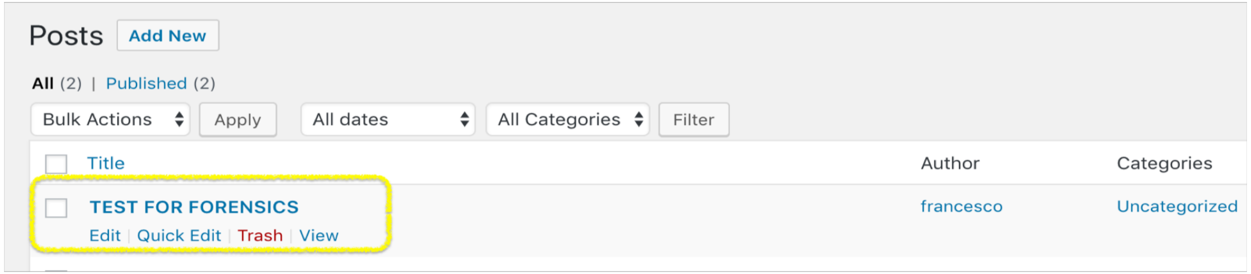
Binary Log

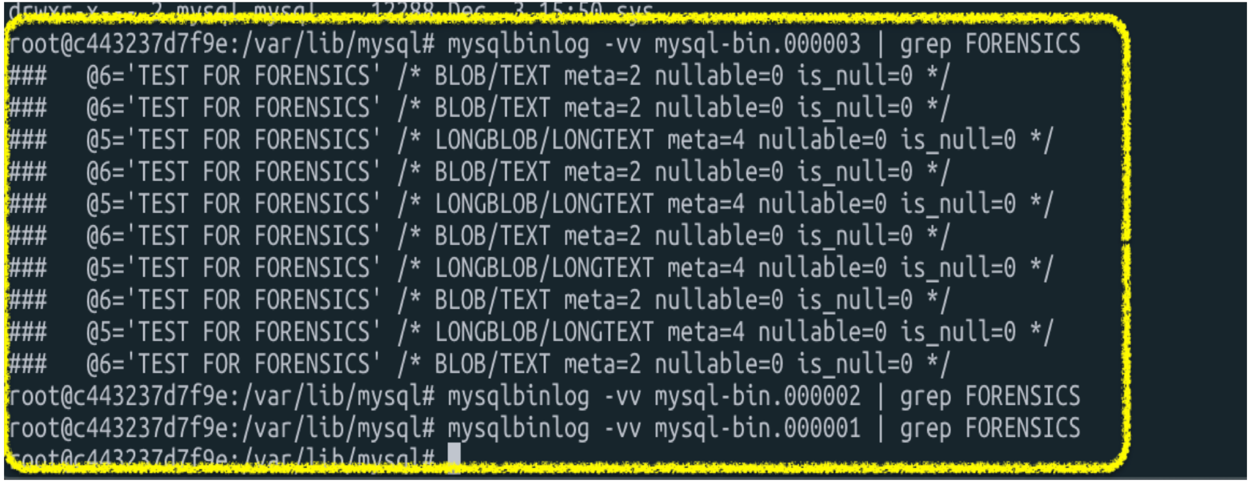
```
root@ip-[redacted] ~francesco/WORK/Docker/web_mysql_compose cat docker-compose.yml
version: '2'

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=[redacted]
                        - 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@[redacted] ~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

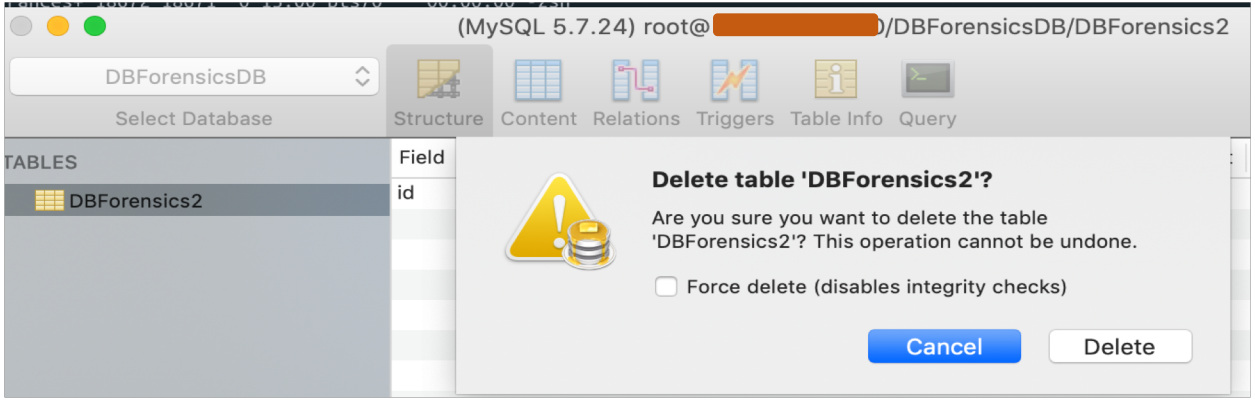
WORDPRESS에서 게시물 INSERT한 내역





DBMS 관리 툴에서 테이블 삭제

Binary Log




```
# at 1499200
#181203 16:18:00 server id 1  end_log_pos 1499336 CRC32 0xeeeedc43      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 0x0d115456      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.