DELETED DATABASE ROWS EXTRACTION FROM DATABASE (MySQL, MSSQL & ORACLE SQL) WITH THE HELP OF COMMERCIAL TOOLS AND TECHNIQUES

[1] Rushabh Ladhani [2] Dr. Priyanka Sharma

[1] Post Graduation, Cyber Security, Raksha Shakti University, Ahmedabad, Gujarat, India

[2]Professor and Head, Information Technology & Telecommunication Department, Raksha Shakti University, Ahmedabad, Gujarat

ABSTRACT

The most problematic thing in the Server Forensic is the Database Forensic. In Database Forensics, Digital Forensic Examiner almost every time receive databases with the deleted entries. Therefore, there are no any evidences can recover from that database because of that main entries of database that can be evidences is actually deleted. So here in this research work using some tools and techniques, we will recover deleted database entries of the MSSQL, MySQL and ORACLE database. This research work put a spotlight on how database with the deleted entries investigated and recover the forensic artifacts from it. Here for the recovery of the database entries we will use the tools like Systools SQL Log Analyzer, Systools SQL Recovery, and Oracle's deleted database entries recovery by logs etc. There are hundreds of hurdles with these tools also. Here we will extract deleted entries from the databases whether it is offline or online by using commercial tools as well as various techniques.

KEYWORDS: Database Forensics, MySQL Forensics, MSSQL Forensics, ORACLE SQL Forensics, Deleted Database Recovery

INTRODUCTION:

In recent times, Deleted Database Extraction is key concept in digital forensic. Every Digital Forensic Examiner is trying to understand the concept behind the recovery of deleted data from database like MSSQL, MySQL, and ORACLE SQL. It poses huge threat to Digital Forensic Examiner. People are becoming smart to protect their unlawful activities, illegal activities, tax evading etc. for their own profit. Traces of this unlawful activity in any database system can identified through Deleted Database Extraction by digital forensic techniques.

Based on my experience as a Forensic Consultant in one of the best organization, I saw many servers and database repository on premise as well as remote servers. In which I found many databases and worked on that. At the time I faced many challenges in databases like someone deleted database as a whole and sometimes I found database rows deleted that is not legitimate. There are many tools that can recover that deleted entries from the database but there are lack of knowledge how to use that tools or without tools how we can see that entries. I also faced these difficulties at the time of analysis of these kinds of database. Therefore, here I found some tools and technique that can recover deleted rows from the database as well as we can see that when it was deleted, updated and inserted.

FORENSIC POINT OF VIEW

Database is backbone of any small to big size organization. We can found everything about the company by just analysing the database. In forensic point of view, we saw that, any organization deleted data by no reason when digital forensic of that organization took place, at that time there are some unlawful activities took place. Like some organization deleted their credit records, sometimes they deleted that dummy and fake transaction records, sometimes we found some money laundering database deleted from the main database, sometimes we found that database as a whole deleted but that can we recover by the deleted data recovery of the systems as a whole. However, after that recovery, in that deleted database also contains some kind of the updated rows and columns, deleted rows and columns, etc. It is one of the point that matters a lot in legal process. Another one is when, any personal deleted database entries as well as modified

database for their own purpose or and hacking activities took place at that time also these approach is beneficial.

Now, by following below steps, we can analyse modified, deleted and other database operation entries.

MySQL

People used to said that NoSQL + SQL = MySQL. MySQL have a large customer base all over the world. MySQL is one of the largest database that uses many big size organizations like e commerce, education institutes, aerospace agencies, defence agencies, financial services agencies, government, pharma healthcare, retail, travel agencies etc.

In MySQL when some database deletion-operation or modification-operation in database took place it records in their own Binary Log Files. Binary logs contains events. Whole database operation we can found in binary logs. Binary logs can found that how long each statements took that updated data.

There are generally two types of binary logs files;

1. Index files – It is a binary log index files. Its extension is (.Index)

   It records all the entries of binary files.

2. Binary Log Files – It is actual binary log file. Its extension is (.000000, .000001, .000002 etc.)

   It records all the logs of data definition language and data manipulation language.

Therefore, here we can analyse impotent deleted in the MySQL by Binlogs. Binlog is primary database forensic investigation tool for MySQL.

For this approach, there is only one condition and that condition all the Database Administrator follows, it is, Binlogs should enable before the database creation. This practice every small to big size organization following because this Binlogs also important for them for the fail over recovery or at the time of sensitive database operation misplaced.

For checking Binlog, enable or not we have to check MySQL configuration file. Its name is my.ini, which is located into the root folder of the MySQL.

C:\Program Files\MySQL\MySQL Server 8.0\my.ini

We can also check by the command line also.

Mysql> show variable like 'log_bin';

It will generate one table and in that table if log_bin is ON, that means MySQL Binlog is enabled.

Another one technique is to check Binlog, check in the storage folders in windows or type in the search bar of the windows explorer. If there are file name like below found it means Binlog is enabled but make sure it should be current database bin log file.

Mysql-bin.000001

Here is the full by default path of the Binlogs:

C:\Program Files\MySQL\MySQL Server 8.0\Data\binlogs

Here we found Binlogs. Now we have to analyse Binlogs, read that Binlogs it is in binary format so we cannot just open it in notepad and read it like a simple file. For reading, this bin logs files we need to open these files within MySQL only.

In this MySQL there are a tool called mysqlbinlog that is located in the below path, go to this path open the command prompt and go to this mysqlbinlog directory and write this query and hit enter.

C:\Program Files\MySQL\MySQL Server 8.0\Data\bin> mysqlbinlog –V "bin log full path paste here"

Binlog file is open now and we can analyse it properly with time & date and which query was fired that is also we can see that and by this we can find that, what data is deleted from the MySQL database.

ORACLE SQL

Oracle database is the one of the major database services providers who are providing huge variety of database services for small to bigger size organizations. [1] Oracle gets 80% of its revenue from the Fortune 2000 companies and various government agencies. They do sell to thousands (or hundreds of thousands) of customers. Some of them are US Federal Government and its agencies like the DOD, Mineral Technologies, Apollo Group, Apple Inc., BT, Verizon, P & G, National Instruments, Hyundai, Airbus etc [1].

Here in ORACLE SQL, when some database modification or deletion operation performed it is also save in their redo logs and archive logs. In redo logs, it is by default save their entire database operations save and for archive logs we have to enable that archive logs before creating database or at the designing time of database. Redo logs only have some information of that database its usually work in LIFO fashion.so it does not have long history of database operations but in archive logs it Is have all the history of the database. At the configuring time of archival logs of the database, needs to create how much MB's or GB's of archival logs want to create or how much and where you want to store that archival logs in the system generally its save in the flashback directory.

Redo log path by default: **c:\\app\rushabh\oradata\orcl\Redo01.log**

For the recovery of the deleted data and modification done in database we have to configure flash recovery area. Flash recovery area is by default off in the system. But usually when the database administrators create and design that database at that time they also configure this flash recovery area because when sometimes by mistake any deletion query run without where clause it creates huge mess. For this type of solve this types of hurdles they needs to configure flash recovery area into the database.

Steps to create flash recovery area in database:

Where you want to save your flash recovery area folder at that place, create the folder of flash recovery area. Note this it will consume big space parallel to database grows. After creating this folder, open SQLPLUS from the start menu it will open window like command prompt or we can open cmd and write as like below.

Login into the SQLPLUS as SYSDBA.

C:\Users\rusha> SQLPLUS /as sysdba

After login into the sqlplus, need to provide the size of the flash recovery area here its 12 gb.

SQL>ALTER SYSTEM SET db_recovery.file_dest_size = '12g';

After this need to provide the destination of the flash recovery area.

SQL> ALTER SYSTEM SET db_recovery.file_dest = 'copy and paste here flash recovery area folders full path';

Now shutdown the database and open again.

SQL>SHUTDOWN IMMEDIATE;

SQL>STARTUP MOUNT;

It also needs to archive logs enable so by that can see the changes done in the database.

SQL>ALTER DATBASE ARCHIVE LOG;

[2]Optionally, specify the length of the desired flashback window (in minutes) by setting the **DB_FLASHBACK_RETENTION_TARGET** initialization parameter. The default value for this parameter is 1440 minutes, which is one day. The following command specifies that the flashback window must be 3 days [2].

SQL>ALTER SYSTEM SET DB_FLASHBACK_RETENTION_TARGET = 4320;

SQL>ALTER DATABASE OPEN;

Now by the following query we will generate the list of database archival logs if it configured nicely it will gives you output:

SQL>ARCHIVE LOG LIST;

SQL>SELECT FLASHBACK_ON FROM V$DATABASE;

By default now, flashback window must be 3 days. However, if we want to change flashback window manually, by this we can change it.

SQL>ALTER SYSTEM SWITCH LOG FILE;

Now logs are set this type of configuration already done I found in one of my case. Every organization, who uses this oracle database they always configure this type of database configuration for the failover recovery or point in time recovery.

Now when some forensic analysis took place at the time if you found database as oracle then need to first check in the sqlplus that if it have archive mode on or not. In 99.99%, it is always enabled. So, login into sqlplus as sysdba and give following query.

SELECT LOG_MODE FROM V$DATABASE;

It will show you log mode archive mode in the output. Now we need to open logminer in the oracle database they provide tool with the installation time of the database it is database control tool from the start menu. It will open the Oracle Enterprise Manager. Log in to the OEM as a sysdba.

Go to **availability tab**, select **view and manage transaction** under **manager** now logminer is open in front of you. However, before we go to next step we need to configure supplemental logging. Because for using logminer, database must has, least minimal supplemental logging enabled. Therefore, for this we need to open sqlplus from the start menu and login as a sysdba and fire following queries:

SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA;

SQL> SELECT SUPPLEMENTAL_LOG_DATA_MIN FROM V$DATABASE;

Now open the OEM and go to **view and manage transaction**, it will open the logminer window. Select the date and time range between that time and date range you want to see logs. Here select that date and time segment in which may be some deleted or modified some data or rows or columns and select a particular user otherwise it will select by default and press continue.it will gives you list of transaction logs with the name of DB users and time date columns. Select the view by redo record. Therefore, it will shows you the query that fired. So go to transaction id and select one of them it will take you to the another page called transaction details and there you can see whole things and you can recover that transaction after commit the transaction also by clicking on the flashback recovery and in the next confirming page clock on yes. Here if you are recovering first time data by the use of flashback then you need to add supplemental log data column and assign primary key to this.

SQL>ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;

After this click on **flashback transaction** and say yes on confirming page, it will recover your deleted or modified data.

MICROSOFT SQL SERVER

[3]In Microsoft SQL Server usage, India is on the third number as per the report of idatalabs. So many industries in various sector using Microsoft SQL Server. Like, Computer Software Information Technology and Services, Hospital & Health Care, Financial Services, Higher Education, Retail, Computer Hardware, Construction, Management Consulting, Insurance etc [3].

Comparatively, Microsoft SQL Saver's deleted database rows analysis is easier then ORACLE SQL and MySQL. Whenever you delete something from the Microsoft SQL Server, it will save this transaction in its logs called LDF file. LDF is just a file extension for a log file, which used in Microsoft SQL Server. In addition, it includes, logging information all the transaction done by the Microsoft SQL Server. By the use of LDF, files easily recover any transaction to the Microsoft SQL Server.

In Microsoft SQL Server MDF and LDF, files are located at below path in my case. It always with its MDF files. MDF files are the database file. It contains database of the Microsoft SQL Server. Both files found on below path:

C:\Program Files\Microsoft SQL Server\MSSQL10_50.diss\DATA

Therefore, we found log files of the Microsoft SQL Server. Now we insert that log files into Systools Log Analyser Tool. Open that ldf file and analyse each transaction. If any of the transaction made then it saved into this log files. It is not only records delete and update logs. It also includes insert, joint, view, redo, undo, every types of transaction it saves in to their logs. So open that logs into the tool and when any illegitimate entries found, click on that entry and go to details view inside this can see all queries that user had done with the proper time and date.

CONCLUSION

Database is the most sensitive part in information technology era. In this time as per forensic point of view, database forensic is tuff. It contains so many possibilities and hurdles. However, in some cases in some scenarios we can recover database as a whole, deleted rows of that database or any transaction that made by any personal. In this paper we discussed 3 SQL Databases and seen that Microsoft SQL Server database have a large possibilities as compare to all because there are no any dependencies like oracle. We just need to collect ldf file and view. After this MySQL is the second database that, not having hurdles like Oracle SQL Database have and third one is the Oracle SQL Database, which have many dependencies for the recovery of deleted and modified transactions.

FUTURE SCOPE

Here, I listed the techniques for Microsoft SQL Server, MySQL Server and Oracle SQL Server to recover and analyse deleted rows and modified transactions. In future, we can find and use these types of techniques for further databases like SQLite DB, FoxPro DB, IBM DB2, Sybase etc.

REFRENCES

1. https://www.quora.com/What-does-Oracle-sell-and-who-are-its-target-customers
2. https://docs.oracle.com/database/121/ADMQS/GUID-2598AA28-DBBB-4B40-AABC-B28FB5C5F4BE.htm
3. https://idatalabs.com/tech/products/microsoft-sql-server