

Forensic Analysis of Database System

Mr Ashwin M. Makwana¹, Director Dev M. Rathod²

¹ PG Student ² Director

¹CE Department Gujarat Technological University. Ahmedabad.

²Prediqnous Cyber Security And I.T Intelligence. Ahmedabad City.

Abstract--The current scenario of Digital world is different than as it was before 5 years. Cyber Crime activities are at its high and hence IT security field has really picked up. Almost every week, you will hear at-least one report of intrusion on database of any company. IT security experts and forensic Investigators have found it very complex when attack is on any SQL server database. When the security of an SQL server database is compromised, In few case forensic investigators are unable to qualify or assess the scope of the intrusion. In such cases, they have to publicly report the damage. This is difficult not only for customers but for companies as well, who have to risk their reputation and brand image. To avoid this type of accident, the best way is to master specialized skills required to deeply investigate intrusions on SQL Server. There are many existing technologies are there to analyze and investigate the compromised SQL Server Database. In this Dissertation, I will present very effective and novel approach of Digital Forensic Investigation, which will present that how to gather and preserve database artifacts security and without any disruption. Then I will be proposing model to perform in-depth analysis to verify and analyze any database intrusions very effectively. This model will expose the activities of the intruder in database server. This model will be used to determine unauthorized data access or modification as well as to collect information required for database recovery by restoring to an earlier state.

Keywords: forensics, database, attacks, analysis, evidence, anti-forensic.

I. INTRODUCTION

In a digital age, information has become an important resource that people depend on in every aspect of their lives. With the use of computers and networks, the communication of information becomes more faster. Fast internet makes it possible to create social networks and share news and events across the world quickly. However, as people enjoy the convenience of information access and transfer, the risks of privacy problems and security increase greatly too. People with malicious motives use different technology as a tool to access information they are not authorized to access. With these malicious actions computer and network forensics emerged as a discipline.[4]

Database hacking has gone mainstream and is becoming hard to detect because of the increasingly sophisticated anti-forensic procedures hackers use to cover their tracks harder.

Our aim to make an accurate forensic Model, which will analyzing or examining data to discover evidence, presenting the evidence to the court and doing all this within the scope of various laws.

II. BACKGROUND

Data recovery and computer forensics are two separate fields, with differing standards, but sometimes utilizing the

same tools and processes. A computer forensic examiner obtaining evidence that might be presented before a court of law and the word forensic is used to describe that process. Computer forensic examiner will be reviewed by many people so it must be of the highest quality, it must be repeatable and it must be accurate. Computer forensics can be defined as collecting computer data securely and accurately, analyzing or examining that data to discover evidence, presenting the evidence to the court and doing all this within the scope of various laws.[7]

A. Digital Forensic Analysis:

Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, related to computer crime. The word digital forensics was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing data. Digital forensics investigations have a variety of applications.

The most common is to support or refute a hypothesis before criminal or civil (as part of the electronic discovery process) courts. Forensics may also take place in the private sector; such as during internal corporate investigations or intrusion investigation (a specialist probes into the nature and extent of an unauthorized network intrusion).

The technical aspect of an investigation is further divided into several sub-branches, related to the type of digital devices involved; network forensics, computer forensics, database forensics and mobile device forensics. The general forensic process encompasses the seizure, forensic imaging (acquisition) and analysis of digital media and the production of a report into collected evidence.

As well as identifying direct evidence of a crime, digital forensics can be used to feature evidence to suspects, confirm statements, determine intent, identify sources (for example, copyright cases), or authenticate documents. Investigations are much broad in scope than other areas of forensic analysis (where the usual aim is to provide answers to a series of simpler questions) often involving complex time-lines or hypotheses.[4]

B. Database Forensics:

Database forensics is a branch of digital forensics relating to the forensic study of databases and its metadata. Computer Investigators use database log files, data contents and RAM data to make a timeline or recover relevant information.[10]

Database Forensics is a branch of digital forensic science relating to the forensic study of databases and their related metadata. This is same as computer forensics, following the general forensic process and applying investigative techniques to database contents and metadata. Cached information may also exist in servers RAM requiring live analysis techniques.

A forensic examination of a database may relate to the timestamps that apply to the update time of a row in a relational table being inspected and tested for validity in order to verify the actions of a user. Indirectly, a forensic examination may focus on identifying transactions within a database system or application that indicate evidence of fraud.

Third party software tools which provide a read-only environment can be used to analyze and manipulate data. These type of tools also have audit logging capabilities which provide documented proof of what tasks or analysis a forensic examiner performed on the database.

Database hacking has gone mainstream and is becoming harder to detect because of the increasingly sophisticated anti-forensic procedures hackers use to cover their tracks. Databases contain a high percentage of confidential data, many organizations have lack of budget and management buy-in to implement protections. According to studies, 60% of organizations have experienced a breach in the past 12 months, 80% expect database attacks to increase and 40% on average fail security audits.[3]

III. PROPOSE TECHNIQUE

Research on this topic has been in very dark as no proper framework and tools are available for it. In this project dissertation we are focusing on the reliable framework for the database forensic.

Forensic model comprises of mainly five processes. Those are 1. Preparation, 2. Collection, 3. Examination, 4. Analysis and 5. Report.

In my proposed Database Forensic Model, each forensic process will get ahead one by one to achieve the evidence from database residing on the server. In the following explanation, I will brief the each forensic process of my proposed database forensic model.

A. Preparation:

This is the first step of the any forensic investigation in which Investigator needs to understand the nature of the case in hand. Investigator must carry out the conclusion that whether the case is of Law Enforcement or corporate. It is also essential to carry out the conclusion that whether Investigator in-charge will need Database Expert for forensic investigation purpose in examination part of the model. In-charge officer have to identify the team members for the investigation. He also has to deal with applicable laws and policies related with the case. After going through all such formal process, In-charge officer should take the authorization from the decision makers for the acquisition of the database source.

B. Collection:

In this part of the model, investigator has to take the image of the database source with forensically sound acquisition tools. Some of examples of such tools are FTK (Forensic ToolKit), Encase, The sleuth Kit. Investigator needs to take the image in proper format. It may be dd , proprietary or application oriented format based on the tool you use.

Acquisition of the Database source should be handled very carefully. You should not violate the principle 1 mentioned previously. You may also require to take image of the other files or partitions for the investigation purpose.

After taking image of the database source, it must be preserved from any internal or external factors which may damage it.

C. Examination:

In this process, all the MySQL database artifacts are examined to check type of information stored on in that. Architecture of the MySQL dataset is shown in figure 4.1

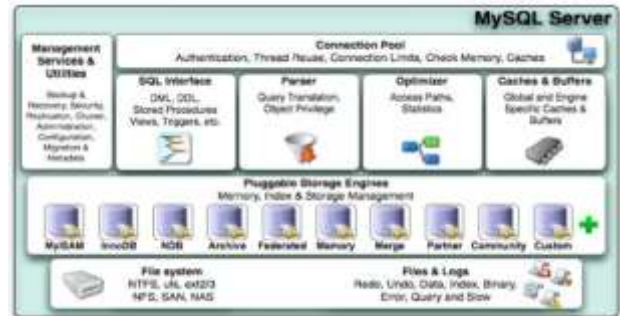


Fig. 1: MySQL Architecture with Pluggable Storage Engines

In this forensic process we will examine the artifacts of the MySQL Database to get the evidence of tampering or other type of attacks. Figure 3 shows them. Following are some of them.

- Information Schema
- MySQL Status and Log Files
- Query Cache
- Other Cache
- Triggers
- Data Files
- Audit Files
- Application Connected with MySQL Database

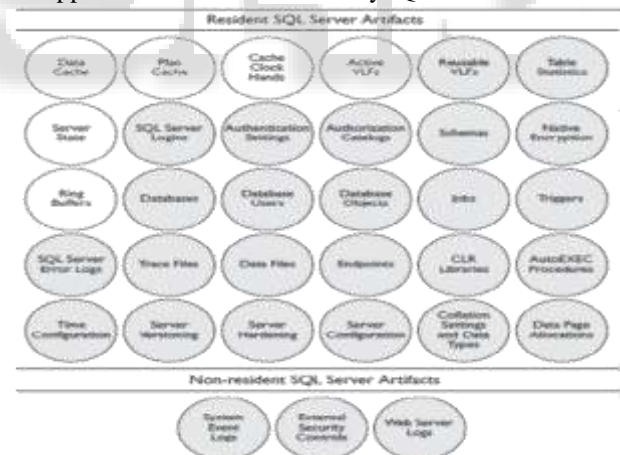


Fig. 2: Artifacts of SQL server

D. Analysis:

In this process, we will analyze all the artifacts gathered from the database manually and also with special forensic tools. It is also essential to find out whether the attacker has used anti forensic techniques or not. Existing techniques are not much reliable to spot the anti-forensic techniques in the attack but in this model we will get that with manual auditing of the data files.

E. Reporting:

Forensic reporting is very essential process for any digital forensic examination. Forensic report is to be generated with special application in such a way that the third party can

easily get the finding of the investigation. Each and every tools and techniques used during the forensic investigation must be included in the forensic report. Each process should be written in the report in such a way that if any third party follows the same process, he should get the same result that you have got.

IV. DISCUSSION AND FUTURE WORK

Most organizations would not have a separate policy for forensics, either due to lack of awareness about importance of database forensics or due to budget issues. Thus this paper makes familiar with the concept of database forensics and proposed a framework which builds the expert system for database analysis. To prove in the concept MySQL database is used here. To interpret the data one has to know a lot about the MySQL Internals. Thus we highlighted some artifacts of MySQL from investigation point of view. The problem which persists in auditing system where there is no intelligence built into it can overcome with our proposed framework. It will give add on features to auditing system to built and retrieve meaningful results in quality time. Thus we contend that determining the identity of the user can be revealed through Database Forensics. In this research paper, the framework is proposed for MySQL which would be implemented to generate the reports. Similarly the framework can be modified and reused for the other DBMS with its own identified artifacts.

V. CONCLUSION

Database Forensics is a very new field with little literature and few tools. This project approached its task by identifying various dimensions of Database Forensics. Various methodologies for tamper detection will be implemented to get more accurate & reliable forensic process for Database Investigation. Major challenges are to counter anti-forensic techniques used by the attacker of the database. In a nutshell this dissertation is intended to draw attention towards Database Forensics with the hope of stimulating research in this important area.

REFERENCES

- [1] Ankit Agarwal, Megha Gupta, Saurabh Gupta & Prof. (Dr.) S.C. Gupta, 'Systematic Digital Forensic Investigation Model', International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (1) : 2011
- [2] Harmeet Kaur Khanuja and D.S.Adane, 'A FRAMEWORK FOR DATABASE FORENSIC ANALYSIS', An International Journal (CSEIJ), Vol.2, No.3, June 2012
- [3] Patrick Stahlberg, Gerome Miklau, and Brian Neil Levine, 'Threats to Privacy in the Forensic Analysis of Database Systems', University of Massachusetts, Amherst.
- [4] Kyriacos E. Pavlou and Richard T.Snodgrass, 'Forensic Analysis of Database Tampering', University of Arizona.
- [5] Harmeet Kaur Khanuja and D .S. Adane, 'Database Security Threats and Challenges in Database Forensic: A Survey', 2011 International Conference on Advancements in Information Technology With workshop of ICBMG 2011.

- [6] Emil Burtescu, 'DATABASE SECURITY - ATTACKS AND CONTROL METHODS', Journal of Applied Quantitative Method.
- [7] O.M. Fasan and M.S. Olivier, 'On Dimensions of Reconstruction in Database Forensics', Proceedings of the Seventh International Workshop on Digital Forensics & Incident Analysis (WDFIA 2012)
- [8] Rami Samara and Brajendra Panda, 'Investigating the Effect of an Attack on a Distributed Database', Proceedings of the 2006 IEEE Workshop on Information Assurance United States Military Academy, West Point.
- [9] Peter Frühwirt, Markus Huber, 'InnoDB Database Forensics', 2010 24th IEEE International Conference on Advanced Information Networking and Applications.