DATA ACQUISITION METHODOLOGY FOR DATABASE FORENSIC

S.D.D.S. Senarath

A dissertation submitted in partial fulfillment for the requirements for
MSc in Cyber Security and Forensics

Department of Computing
Informatics Institute of Technology, Sri Lanka
in Collaboration with
University of Westminster, UK

2020

Abstract

The database crimes are increasing day by day and there is a large number of harmful incidents have occurred due to the database attacks. The large organizations have lost their profits and reputation because of these incidents. These crimes harm the confidentiality, integrity, and availability of database systems. The traditional database security mechanisms do not ensure the accuracy of data protection and that is why database forensic is much important for an organization. Then the evidence of the crimes should be identified and collected accurately, and the table records should not be tampered. Therefore, a data acquisition method should be required in database forensic to retrieve the evidence without any harm to the actual database records.

This research was conducted to find an accurate data acquisition method to collect the evidence in database forensic without tampering the table records. A survey using a questionnaire was conducted with the participation of experienced employees related to database administration and system engineering from different organizations. Interviews were also held with industry experts and gathered information regarding data acquisition in database forensic. An experimental analysis was done using the identified steps of the new data acquisition method in a real time environment using the resources of an organization and with the instructions of some industry experts.

After the analysis of the survey results, interview results and the experiment conducted within a real environment, the framework for the data acquisition methodology was created and identified the steps for the data acquisition in detail. According to the survey results the data acquisition method is mainly required for large organizations who are handling large volumes of data and most of the organizations are related to finance and banking sectors. The framework was designed and developed specially for Oracle databases. This data acquisition method allows to gather evidence and report to the relevant legal parties without tampering the original data or table records.

Keywords: Database Forensic, Data Acquisition