분석 목적별 분류 기반의 데이터베이스 포렌식 모델

김성혜[O1] 김장원[2] 백두권[2]
[1]고려대학교 소프트웨어공학과
[2]고려대학교 컴퓨터전파통신공학과
{kimsh96[O], ikaros1223, baikdk}@korea.ac.kr

A Aim of Analysis based Database Forensic Model

SungHye Kim[O1] Jangwon Kim[2] Doo-Kwon Baik[2]
[1]Dept, of Software Engineering, Korea University
[2]Dept, of Computer Science & Radio Communications Engineering, Korea University

1. 서 론

디지털 포렌식은 디지털 포렌식의 프로세스 모델에 대한 연구와 디지털 포렌식 분석으로 나눌 수 있다. 디지털 포렌식의 프로세스 모델에서는 증거를 수집하고 분석하는 디지털 포렌식의 표준화 및 디지털 조사 프로세스에 대한 연구가 있다 [1, 2]. 디지털 포렌식 분석에 대한 연구는 디스크 포렌식, 운영체제에 따른 시스템 포렌식, 인터넷 포렌식, 네트워크 포렌식, 데이터베이스 분석으로 세분화되어 연구되고 있다 [3, 4]. 디지털 포렌식 분석에 대한 연구 중 데이터베이스 포렌식이란 데이터베이스와 관련된 전반적인 분석으로, RDBMS 소프트웨어에 적용하여 복원하고 분석 시 적용할 수 있다 [5].

현재 디지털 포렌식 분석을 위한 프로세스 모델이 다양한 분야별로 연구되고 있지 않기 때문에 데이터베이스 포렌식 분석을 위한 정형화거나 또는 일반화된 프로세스 모델이 없는 문제점이 있으며, 특정 벤더나 제품에 국한된 연구 [6, 7, 8, 9, 10]가 주로 이뤄지고 있기 때문에 특정 데이터베이스의 물리적인 구조에 종속적이라는 문제를 가진다.

또한 기존의 데이터베이스 포렌식 기법에서는 분석대상을 분석 목적 기반으로 분류를 하고 있지 않다. 그러므로 데이터베이스 포렌식에서는 상황별 특징에 따라 적용 가능한 모델이 필요하지만 현재는 이러한 모델들이 없는 상황에서 분석이 이뤄지고 있다. 이런 문제로 인해 각 상황별로 분석 목적에 따라 분석할 수 있는 공통 모델에 대한 연구가 필요하게 되었다. 이 논문에서는 기존의 문제점을 해결하기 위해 분석 목적별 분류에 따른 데이터베이스 포렌식 모델(DFM)을 제안한다.

2. 본론

현재 디지털 포렌식의 분석 프로세스에 대한 연구는 DFRW(Digital Forensic Resarch Workshop) [2]이 있으며 데이터베이스 포렌식에 대한 연구는 Patrick의 database analysis [10]등이 있다. 하지만 DFRW에서는 디지털 포렌식에 관한 전반적인 절차에 대해 설명하고 있으며 Patrick은 데이터베이스 포렌식의 분석방법 중 일부를 설명하고 있다. 그러므로 데이터베이스 포렌식의 분석 모델에서부터 분석 방법까지, 데이터베이스의 벤더에 종속되지 않고 분석 상황별로 분석대상의 목적에 따라 적용시킬 수 있는 새로운 데이터베이스 포렌식 분석 방법론이 필요하다.

제안하는 데이터베이스 포렌식 모델(DFM)에서는 데이터베이스의 분석 목적에 따라 네 가지로 분류하고 각 분류별 분석절차를 다르게 적용하는 모델을 제안한다. 분류에 해당 하는 분석절차를 17개의 프로세스로 나누고, 각 프로세스는 고유한 번호를 부여하여 상황별 목적에 따라 프로세스를 선택 및 배열하고 있다.

첫 번째, DBMS를 통한 분석은 피해 데이터베이스 서버를 분석하거나 별도 분석용 데이터베이스 서버를 구축하여 분석한다. 이것은 불법적인 데이터베이스 서버의 운영이나, 경영자료, 회계 자료와 같은 특정 데이터의 증명 시 적용 할 수 있으며, 또한 서버가 해킹을 당했을 경우에도 적용 할 수 있다.

분석용 데이터베이스 서버를 구축할 때는 원본 데이터베이스에서 데이터파일, 로그파일, 시스템 파일을 가지고 복원하거나 백업된 데이터를 분석용 데이터베이스 서버에 복원하여 분석한다. 또한 해킹을 당했을 경우는 시스템 파일 분석에서 운영체제 로그나 데이터베이스 로그 또는 레지스트리 등을 통해 분석한다.

두 번째, 소스를 통한 분석 방법은 데이터베이스 서버나 백업본 뿐만 아니라 실제 사용하고 있는 소스

를 동시에 분석하는 것이다. 이럴 경우 '데이터를 어떻게 가공 하느냐'가 중요한 문제이다. 소스분석을 하고 테이블 데이터 간의 관계를 분석하고 SQL을 조립해 필요한 데이터들을 추출한다. 데이터베이스에 접속하기 위해 대부분의 프로그램들이 사용하는 파일뿐만 아니라, 소스파일을 통해서 데이터베이스에 있지 않은 내용까지 분석이 가능하다.

세 번째는 데이터베이스 파일을 통해 데이터를 분석하는 방법으로, 데이터 파일이나 로그 파일이 덮어쓰여 정상적으로 복원이 불가능한 경우, 혹은 데이터파일이나 로그파일 중 하나만 있는 경우 파일을 통해 분석할 수 있다. 또 데이터베이스 서버의 복원을 통해서는 삭제된 데이터를 추출할 수 없기 때문에 필요에 따라서는 정상적인 데이터 파일도 분석할 수 있다. 또한 데이터 파일 뿐만 아니라 백업 파일과 로그파일의 키워드 검색을 통해서도 분석할 수 있다.

마지막으로 현장에서의 데이터 수집 및 분석은 현장에서 직접 자료를 추출하는 방법이다. 현장에서 데이터를 추출하는 절차와 시스템 분석표를 작성하여 보관방법을 기재함으로써, 데이터베이스 포렌식의 모델을 마무리한다. 현장에서는 데이터를 수집할 데이터베이스 서버를 선별하는 것이 중요하며, 선별된 데이터베이스 서버에서 시스템 분석 및 각종 로그 분석을 통해 연결된 또 다른 데이터베이스 서버에 대한 정보를 확인할 수 있다. 데이터들을 샘플로 추출한 후 서버 관리자에게 확인할 수 있는 정보가 있으면 데이터들을 확인하여 수집하도록 한다.

실험을 통해 DBMS 분석과 소스를 통한 분석 중 분석 절차에 따라 여러 벤더에서 일정한 절차를 통해 관계분석으로 데이터의 추출이 가능하고, 또 파일을 통한 분석 중 데이터 파일을 통해서 별도 데이터베이스 설치 없이 삭제된 데이터나 손상된 파일에서도 데이터의 추출이 가능하다.

결론적으로 데이터베이스 포렌식은 벤더에 따른 분석방법이 아니라 목적별 분류가 가능하기 때문에 목적별 분류에 따른 분석 절차를 통해 분석하는 것을 제안하고 증명한다.

3. 결론

데이터베이스가 디지털 포렌식에서 한 분야로 분류가 되어 있지만 아직 특정 벤더에 종속적이며 파일시스템에 국한되어 연구가 진행되고 있는 문제점이 있다. 데이터베이스 분석에서 어떻게 데이터들의 관계를 유추하고 필요한 데이터들을 추출 할지에 대한 연구가 필요하며 이 논문에서는 데이터들의 관계를 추출함에 있어서 분석 목적별 분류로 1차 분류를 하고 분류된 모델에 따라 모델별 분석 절차를 가지고 2차 분석을 하도록 제안하고 있다. 제안 DFM을 통해 특정 벤더에 종속적이지 않고 어떻게 데이터들의 관계를 추출할 수 있는지 증명하였다. 현재 데이터베이스 포렌식 분야에서 일반적으로 사용될 수 있는 프로세스 모델 및 분석기법에 대한 연구는 현재까지 진행되지 않고 있지 않기 때문에 제안 논문을 통해 이런 문제를 해결할 수 있다.

이 논문에서는 기존 연구와는 다른 접근방식으로 데이터베이스 포렌식 분석 방법에 적용하여 분석의 편리성, 정확성을 향상시켰으며, 향후에는 각 프로세스별로 더욱 상세하게 적용시켜 상황별 최적화된 분석 방법을 정의하고자 한다.

참고문헌

[1] Gary L Palmer. "A Road Map for Digital Forensic Research", Technical Report DTR-T0010-01, Report for the First Digital Forensic Research Workshop(DFRWS), 2001.

[2] Venansius Baryamureeba, Florence Tushabe, "The Enhanced Digital Investigation Process Model", Digital Forensic Research Workshop, 2004.

[3] Ed Crowley, "Computer Crime and Forensics". http://isacahouston.org/

[4] Gregory S. Miles, "Computer Forensics: A Critical Process in your incident response plan", BlackHat Europe Briefings, 2001.

[5] Database Forensics, http://en.wikipedia.org/wiki/Database_Forensics

[6] David Litchfield, "Oracle Forensics Part 1: Dissecting the Redo Logs", March 2007.

[7] David Litchfield, "Oracle Forensics Part 2: Locating Dropped Objects", March 2007.

[8] David Litchfield, "Oracle Forensics Part 6: Examining Undo Segments, Flashback and the Oracle Recycle Bin", 2007.

[9] Kevvie Fowler, "SQL Server Database Forensics", Balckhat USA briefings and training 2007.

[10] Patrick Stahlberg, Gerome Miklau, and Brian Neil Levine, "Threats to privacy in the forensic analysis of database systems", Proceedings of the 2007 ACM SIGMOD international conference on Management of data, pp. 91~102, 2007.