Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.5, Oct. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.5.1099

윈도우 시스템에서 사용되는 회계 프로그램의 특성을 이용한 포렌식 어카운팅 기법 개선 방안

이 승 주,† 이 국 헌, 이 상 진‡
고려대학교 정보보호연구원

Improvement Method of Forensic Accounting Using Characteristics of Accounting Programs Used in Windows System

Seung-ju Lee,† Kuk-heon Lee, Sang-jin Lee‡
Center for Information Security Technologies, Korea University

요 약

기업에서는 대용량 회계 데이터를 처리하기 위해 각기 다른 회계 프로그램들을 사용한다. 회계 프로그램의 특성으로 인해 회계 프로그램이 사용하는 회계 데이터 이외에도 회계 부정을 탐지하는데 도움이 되는 다양한 정보들이 존재한다. 기존 포렌식 어카운팅 기법은 이러한 정보를 활용하지 않고 회계 원장과 같은 회계 데이터만을 분석했기 때문에 분석할 수 있는 범위에 제한이 있다. 회계 부정 탐지 시, 회계 프로그램의 특성으로 인해 얻을 수 있는 정보들을 활용한다면 회계 데이터 분석만으로는 얻을 수 없는 다양한 정보들을 얻을 수 있다. 본 논문에서는 윈도우 시스템에서 사용되는 회계 프로그램의 특성으로 인해 얻을 수 있는 기타 데이터를 활용하여 회계 부정을 효과적으로 탐지하는 기법을 제시함으로써 효과적인 회계 부정 수사에 기여하고자 한다.

ABSTRACT

Enterprises use different accounting programs to process vast amounts of accounting data. Due to the characteristic of the accounting program, in addition to the accounting data used by the accounting program, there is a variety of information to help detect accounting fraud. Existing forensic accounting techniques have limited scope of analysis because they analyze only accounting data like accounting ledger without using such information. When you do accounting fraud detection, information obtained from characteristics of accounting program can be used to obtain various information that can not be obtained by accounting data analysis alone. In this paper, we try to contribute to effective accounting fraud investigation by suggesting a technique to effectively detect accounting fraud by using other data obtained from characteristics of accounting program used in Windows system.

Keywords: Forensic accounting technique, Accounting fraud investigation, Accounting fraud suspicion scenario

I. 서 론

현재 기업에서는 방대한 양의 회계 데이터를 처리하기 위해 다양한 회계 프로그램들을 사용하고 있다. 회계 데이터가 전산화 되면서 회계와 관련된 일자, 금액, 계정과목 등과 같은 기본 회계 데이터 이외에도 전표 입력한 시간, IP 주소, 사용자 등과 같은 정보를 추가로 얻을 수 있게 되었다. 회계 원장을 이용한 회계 부정을 탐지하는 연구는 활발하지만 앞서 언급한 추가 정보를 활용한 수사 기법에 대한 연구는 미흡한 실정이다.

Received(08. 07. 2017), Accepted(09. 22. 2017)
† 주저자, juiceheaven@naver.com
‡ 교신저자, sangjin@korea.ac.kr (Corresponding author)

현재 전 세계에서 상용되고 있는 회계 프로그램들은 윈도우, 리눅스 등 다양한 운영체제 시스템 환경에서 운영되고 있다. 그러나 윈도우 시스템의 점유율이 타 운영체제에 비해 월등히 높은 만큼[1], 상용 회계 프로그램의 대부분이 윈도우 시스템 환경에서 운용되고 있다. 따라서 효과적인 포렌식 어카운팅을 수행하기 위해 윈도우 시스템 환경에서 동작하는 회계 프로그램들에 대한 연구가 필요하다.

본 논문에서는 윈도우 시스템에서 사용되는 회계 프로그램의 특성을 분석하고, 분석된 결과를 바탕으로 회계 부정 탐지에 도움이 될 수 있는 데이터들을 판별해서 이를 활용할 수 있는 포렌식 어카운팅 기법을 제시한다.

II. 관련연구

2.1 회계 프로그램 구조 분석의 필요성

회계 부정 수사를 위해 데이터를 압수하는 과정에서 회계 원장, 재무제표와 같은 데이터는 회계 프로그램 실행을 통해 얻을 수 있으나, 회계 프로그램에서 보여주지 않는 기타 정보들은 회계 프로그램 실행만으로 얻는 것이 불가능하다. 이러한 기타 정보들을 얻기 위해서는 회계 프로그램이 사용하는 데이터 구조 분석을 통해 필요한 데이터를 추출해야 한다. 따라서 필요한 데이터를 추출하기 위해 회계 프로그램이 사용하는 데이터들이 어떤 식으로 저장되는지에 대한 구조 분석이 필요하다.

2.2 데이터베이스 복구

회계 프로그램은 일반적으로 대용량의 회계 데이터를 관리하기 위해 데이터베이스에 데이터를 저장한다. 데이터베이스의 특성상 레코드를 삭제해도 미할당 영역에 남아있는 데이터를 복구할 수 있다[2]. 회계 프로그램마다 사용하는 데이터베이스가 다르지만 데이터베이스의 삭제된 레코드 복구에 대한 연구는 각 데이터베이스 종류 별로 활발히 진행되고 있기 때문에[3,4,5], 사용자 또는 회계 프로그램이 삭제한 데이터를 복원할 수 있는 가능성이 충분하다. 따라서 사용자가 의도적으로 삭제했거나 시스템의 오류로 인해 레코드가 삭제된 경우에도 대응할 수 있다.

2.3 포렌식 어카운팅 연구 동향

공개된 재무제표 분석을 통해 회계 부정 징후를 탐지하는 포렌식 어카운팅 기법을 제시한 연구가 있다[6]. 실제 회계 감사에서 부정탐지를 위해 사용하는 방법인 추세분석, 수직분석, 재무비율 분석을 자동화 해주고 결과를 시각적으로 표현해주는 도구를 개발하였다. 실제 회계 감사에서 사용되는 분석 방법을 자동화 해줬다는 점에서 의미가 있지만, 재무제표 데이터 이외에 다른 데이터를 활용하지 않았기 때문에 분석된 결과의 범위가 좁다는 단점이 있다.

다음으로 시스템에 설치된 회계 데이터를 추출해서 재무제표 생성하고 통계 분석을 통해 회계 부정을 탐지하는 기법을 연구한 논문이 있다[7]. 해당 도구는 국내 환경에 맞는 최초의 포렌식 어카운팅 도구라는 점에서 의미가 있다. 그러나 회계 프로그램의 종류가 매우 다양하기 때문에 해당 논문에서 만들어진 도구가 실제로 사용될 수 있는 환경이 매우 협소하다는 단점이 있다.

위에서 언급한 연구들은 모두 회계 데이터 분석 자동화를 통해 회계 부정 수사에 도움이 되는 것을 목표로 하였다. 그러나 회계 프로그램의 특성들을 충분히 반영하지 못했다는 점으로 인해 분석할 수 있는 데이터의 범위가 좁다는 한계가 있다. 따라서 회계 프로그램의 특징을 이용한 효과적인 포렌식 어카운팅 기법에 대한 연구가 필요하다.

III. 회계 프로그램의 특성 및 구조 분석

3.1 회계 프로그램의 특성

윈도우 시스템 환경에서 운용되는 회계 프로그램들이 운용되는 방식이나 사용하는 데이터베이스의 종류는 차이가 있지만, 회계 프로그램이라는 공통적인 특성으로 인해 데이터를 저장하는 방식에는 크게 차이가 없다.

대용량의 회계 데이터를 처리해야 하는 회계 프로그램의 특성상 대부분의 회계 프로그램은 데이터베이스를 사용한다. 회계 프로그램이 사용하는 데이터베이스 파일들은 회계 프로그램에 등록된 사용자 또는 회계 기수 별로 구분되어 저장된다. 데이터는 회사 정보, 거래 내역 정보, 계정 과목 정보 등을 데이터베이스 파일 또는 데이터베이스 내 테이블 단위로 구분하여 저장하고 이렇게 저장되어 있는 데이터들을

기반으로 회계 원장, 재무제표와 같은 회계 데이터들을 생성한다.

다음으로 회계 프로그램의 특성으로 인해 저장되는 정보들이 존재한다. 회계 프로그램을 사용하기 위해서는 회사 및 거래처 정보를 등록해야 되는데, 이때 회사 및 거래처의 이름, 대표자명 이외에도 대표자의 주민번호, 회사의 주소 및 계좌번호 등이 저장된다. 또한 전표를 입력할 경우 전표를 입력한 담당자, 전표를 입력한 시스템의 IP 주소 등이 저장되기도 한다. 이러한 기타 정보들을 활용한다면 효과적으로 회계 부정 탐지가 가능하다.

마지막으로 레지스트리 값 확인을 통해 프로그램 설치 폴더 등의 정보를 확인하는 것이 가능하다[8]. 프로그램이 설치된 경로는 레지스트리의 'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\' 경로의 키 값을 통해 확인할 수 있다.

3.2 회계 프로그램 구조 분석 및 기타 정보 확인

본 절에서는 국내에서 사용되는 상용 회계 프로그램들의 구조를 분석하고 실제 내부 데이터 확인을 통해 회계 프로그램의 특성으로 인해 남는 기타 정보를 확인한다.

분석 대상 프로그램은 더존비즈온의 SmartA 2.0 Plus(이하 SmartA), 이지판매재고관리2015 스탠다드 버전(이하 이지판매), MAS V2.0(이하 MAS), QmoneyERP(이하 Qmoney), iEnrich (이하 iEnrich) 이다.

Table 1.은 레지스트리 분석을 통해 확인된 회계 프로그램들이 설치된 경로이다. 설치된 경로의 하위에는 Data 라는 이름을 가진 폴더가 존재하거나 데이터베이스 파일들이 존재한다.

Table 2.는 회계 프로그램별로 사용하는 데이터베이스의 종류를 명시해놓은 표이다. SQLite, MongoDB, Microsoft SQL Server 데이터베이스의 경우 삭제된 레코드를 복구할 수 있는 방안에 대한 연구들이 진행되고 있으나[3,4,5] TopSpeed, Firebird 데이터베이스의 삭제된 레코드 복구에 대한 연구는 진행된 사항이 없다. 각 데이터베이스에서 삭제된 레코드를 복구할 수 있는 가능성이 존재하는지 확인하기 위해 회계 프로그램에서 데이터를 삭제한 데이터가 남아있는지 확인하였다.

Table 1. Data path of accounting programs

Name	Data path
Smart A	C:\NIP_DB_Plus\SmartAPlus\
Easypanme	C:\easypanme2015_standard\
MAS	C:\NeoEast
Qmoney	C:\큐머니
iEnrich	C:\iEnrich

Table 2. Database used by accounting programs

Name	Database
Smart A	SQLite (Modified)
Easypanme	MongoDB
Qmoney	TopSpeed
iEnrich	Firebird
MAS	Microsoft SQL Server

TopSpeed 데이터베이스의 경우 데이터베이스 파일 내 레코드는 특정 값으로 덮어써지지만 특정 폴더에 데이터베이스 파일을 백업해둔다. 따라서 원본 폴더와 백업된 파일을 비교함으로써 삭제된 레코드를 판별 및 복구할 수 있다.

Firebird 데이터베이스의 경우 데이터베이스 파일 내에 삭제한 데이터가 잔존한다. 따라서 데이터베이스 구조 분석이 된다면 데이터베이스 내 삭제된 레코드를 복구할 수 있다.

회계 프로그램의 특성으로 인해 저장되는 기타 정보의 경우 조사 대상 회계 프로그램 모두 회사 및 거래처의 이름, 대표자명, 대표자 주민번호, 회사의 주소 및 계좌번호와 같은 회사 및 거래처의 상세 정보를 저장한다. 또한 조사 대상 회계 프로그램 모두 전표 입력 시 담당자의 이름을 적게 되어있다. 이외에도 SmartA의 경우 서버, 클라이언트 환경에서 운영되기 때문에 전표를 입력한 시스템의 IP 주소가 남아있다.

IV. 포렌식 어카운팅 기법 개선 방안

본 장에서는 회계 프로그램의 특성을 이용한 개선된 포렌식 어카운팅 기법을 제시한다. Fig.1.은 본 논문에서 제시하는 포렌식 어카운팅 기법의 구성도를 보여주는 그림이다.

먼저 회계 프로그램의 특성을 이용해서 용의자의 PC에 설치된 회계 프로그램을 식별하고 필요한 데이터를 압수한다. 압수한 데이터는 회계 장부 등과

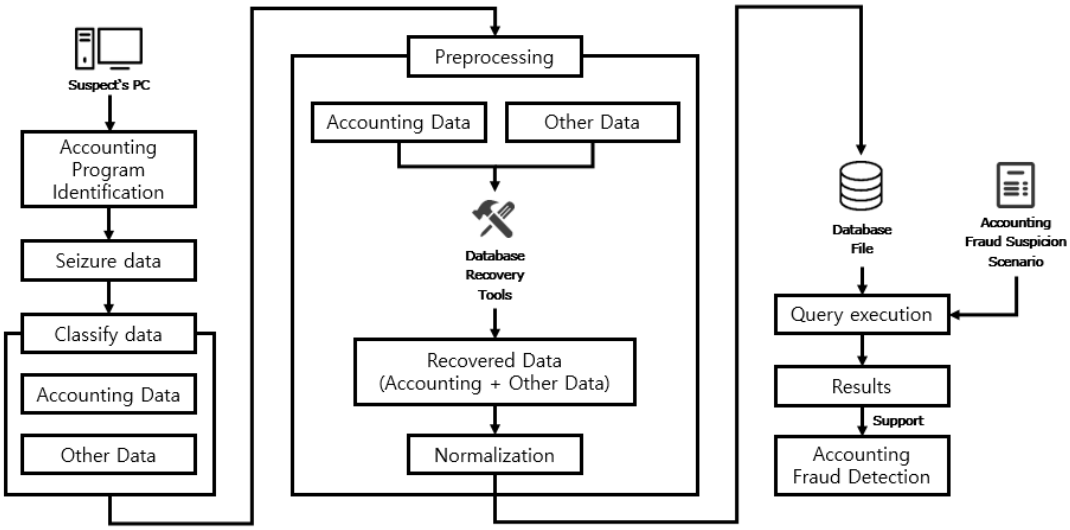

Fig. 1. Forensic accounting technique diagram which is presented in this paper

같은 회계 데이터와 회계 프로그램의 특성으로 인해 남아있는 기타 데이터로 구분한다. 다음으로 각 데이터베이스에서 삭제된 레코드 복구 작업을 수행한다. 삭제된 레코드 복구 작업을 통해 사용자가 의도적으로 삭제한 데이터들을 분석함으로써 추가적인 사용자의 의도를 파악할 수 있다. 삭제된 레코드를 복구했다면 기존에 저장된 데이터와 삭제된 데이터를 조합해서 분석하기 위한 형태로 정제 후 데이터베이스 파일에 저장한다. 데이터를 분석하기 위한 형태로 정제한다는 것은 기존의 데이터에 복구된 삭제 데이터와 회계 프로그램의 특성으로 인해 얻을 수 있는 기타 데이터들을 저장할 컬럼을 데이터베이스에 추가하는 작업을 의미한다.

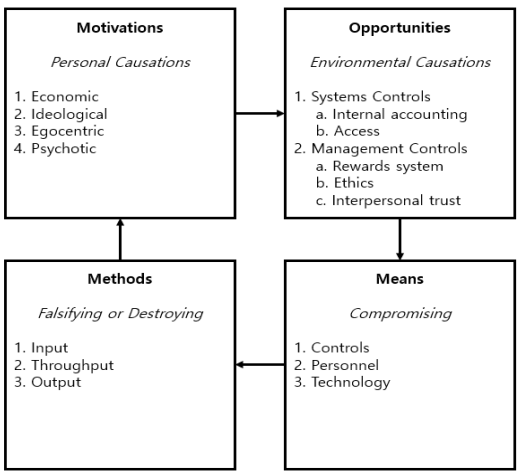

Fig. 2. MOMM theory

분석을 위한 데이터베이스 정제 작업이 완료되었다면 미리 정의한 회계 부정 의심 시나리오가 저장된 쿼리문을 실행한다. 회계 부정 의심 시나리오는 회계 데이터와 기타 데이터를 함께 활용해서 회계 부정이 의심되는 데이터를 탐지하는 내용으로 이루어져있다.

본 논문에서는 회계 부정 의심 시나리오를 작성하기 위해 MOMM 이론을 활용하였다[9]. MOMM은 Motivations, Opportunities, Means, Methods의 약자로 컴퓨터와 관련된 부정 행위는 위 4가지 단계가 순환된다는 이론이다. Fig.2.는 MOMM 이론을 보여주는 그림이다. Motivations는 부정을 저지르는 동기의 종류, Opportunities는 부정을 저지를 수 있는 환경, Means는 부정의 주체, Methods는 부정을 저지르는 행위의 종류를 나타낸다. 회계 부정 의심 시나리오는 MOMM 이론에서 Means, Methods를 활용해서 사람의 행위와 입력된 데이터 분석을 통해 회계 부정 의심 행위를 탐지한다. Table 3.은 본 논문에서 정의한 시나리오들의 목록을 기술해놓은 표이다.

회계 부정 의심 탐지 시나리오를 활용하는 기법은 기존의 포렌식 어카운팅 기법에서는 활용하지 않았던 다수의 유용한 정보들을 동시에 활용하기 때문에 효

Table 3. Lists of accounting fraud suspicion scenarios

Index	Title
1	Lists of general slip which was modified or erased by person who is not in charge.
2	Lists of general slip which was modified or erased at other PC which is not in charge.
3	Lists of general slip which was modified or erased by person who do not input general slip.
4	Lists of general slip which was input or modified or erased at outside of company.
5	Among registered customers, lists of general slip which dealt with customers having same representative.
6	Among registered customers, lists of general slip which dealt with customers having same address.
7	Lists of purchase(or sale) slip which was modified or erased by person who is not in charge.
8	Lists of purchase(or sale) slip which was modified or erased at other PC which is not in charge.
9	Lists of purchase(or sale) slip which was modified or erased by person who do not input purchase(or sale)s.
10	Lists of purchase(or sale) slip which was input or modified or erased at outside of company.
11	Lists of purchase(or sale) slip which dealt with customers which have same representative among registered customers.
12	Among registered customers, lists of purchase(or sale) slip which dealt with customers having same address.
13	Among registered customers, lists of purchase(or sale) slip which dealt with customers having same representative.

과적으로 회계 부정을 탐지하는 것이 가능하다.

V. 개선된 포렌식 어카운팅 기법 활용 방안

본 장에서는 논문에서 제안한 포렌식 어카운팅 기법을 어떻게 활용할 수 있는지 보이기 위해 도구를 구현하였다. 도구에서는 정제된 회계 및 기타 데이터가 저장된 파일을 입력받아 데이터베이스 파일로 만들고 미리 정의해놓은 회계 부정 의심 시나리오를 실행시켜서 결과를 보여준다.

실험에 사용된 데이터는 실제 현장에서 SmartA 프로그램을 사용하는 회사로부터 수집하였고, 회계 부정 의심 데이터가 탐지되도록 내부 데이터를 수정하였다. 데이터베이스의 삭제된 레코드 복구 및 정제는 수동으로 진행하였고 데이터들을 csv 형태로 저장 후 프로그램에 입력하는 과정을 수행하였다. Fig.3.은 프로그램에 csv 파일들을 입력하는 것을 보여주는 그림이다. csv 파일들을 입력한 후 '시나리오 추출' 버튼을 누르면 각 시나리오에 해당하는 데이터들이 출력된다. Fig.4.는 회계 부정 의심 시나리오에 해당하는 데이터들이 출력되는 것을 보여주는 그림이다. 출력되는 정보 중 회사의 직접적인 정보가 나오는 부분은 음영처리 하였다.

구현한 도구에서는 회계 프로그램에 저장되어 있

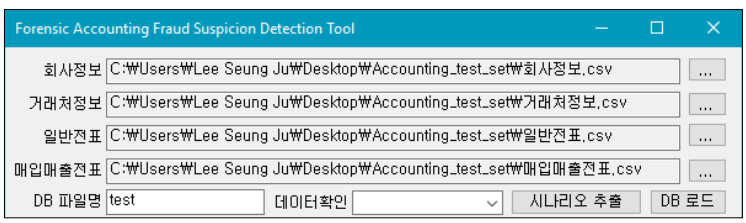

Fig. 3. Insert csv files in tool

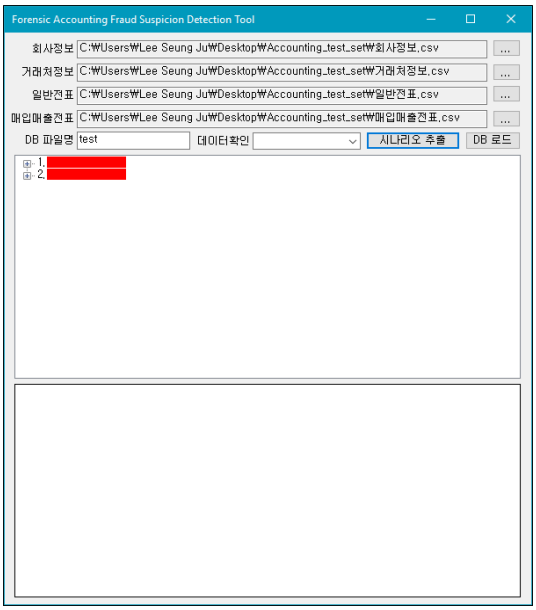

Fig. 4. Results of extraction

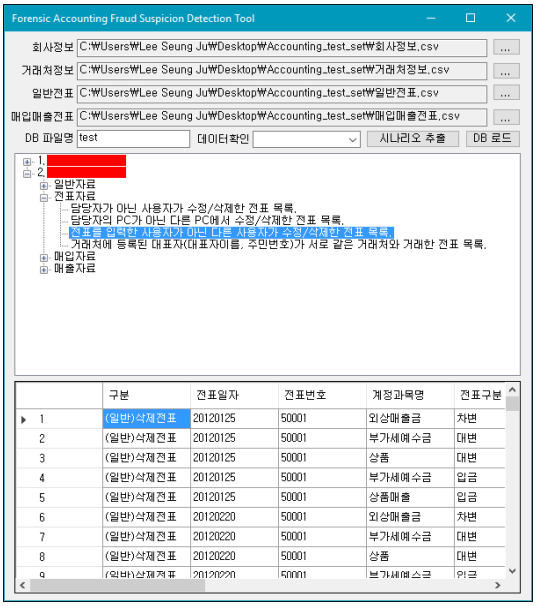

Fig. 5. Results of scenarios

는 회사 코드별로 구분해서 데이터를 보여준다. 실험에서 확인할 수 있듯이 회계 프로그램에 등록된 회사가 2개임을 알 수 있다. '+' 버튼을 클릭하면 탐지된 회계 부정 의심 시나리오 목록이 나오고 시나리오를 클릭하면 해당 시나리오에 대한 자세한 내용이 아래 부분에 출력된다. Fig.5.는 도구에서 출력되는 시나리오를 보여주는 그림이다. 도구에서 출력된 결과를 통해 회계 부정이 의심되는 데이터를 판별할 수 있고 실제 회계 부정 분석 시 분석 범위를 줄여줌으로써 효과적으로 회계 부정 탐지가 가능하다.

VI. 결과 및 향후 연구방향

본 논문에서는 윈도우 시스템에서 사용되는 회계 프로그램의 특성을 분석하고 이를 활용해서 효과적으로 회계 부정을 탐지하는 기법을 제시하였다. 기존에 연구된 회계 부정 분석 방식은 그 범위가 회계 원장과 같은 회계 데이터에만 한정되어 있어 회계 프로그램의 특성으로 인해 존재하는 데이터들을 활용하지 못했다는 한계가 있다.

본 논문에서 제시한 포렌식 어카운팅 기법은 기존 포렌식 어카운팅에서 활용하지 않았던 데이터를 활용해서 회계 부정 의심 데이터를 탐지하기 때문에 회계 데이터만 사용했던 방법에 비해 효과적으로 회계 부정을 탐지할 수 있다는 점에서 의의가 있다.

향후 연구로는 윈도우 환경이 아닌 다른 운영체제 환경에서 동작하는 회계 프로그램 분석을 통해 윈도우 운영체제 이외의 시스템에도 적용할 수 있는 포렌식 어카운팅 기법에 대해 연구할 예정이다.

References

[1] NETMARKETSHARE, "Desktop Operating System Market Share," https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0

[2] Olivier, Martin S, "On metadata context in database forensics," Digital Investigation, vol. 5, no. 3, pp. 115-123, Mar. 2009.

[3] SangJun Jeon, Jewan Bang, KeunDuck Byun, GuenGi Lee, and SangJin Lee, "The Method of Recovery for Deleted Record in the Unallocated Space of SQLite Database," Journal of the Korea Institute of Information Security and Cryptology, 21(3), pp. 143-154, Jun. 2011.

[4] Jong-Seong Yoon, Doo-Won Jung,

Chul-hoon Kang, and Sang-Jin Lee, "Digital Forensic Investigation of MongoDB," Journal of the Korea Institute of Information Security and Cryptology, 24(1), pp. 123-134, Feb. 2014.
〔5〕 Lian, X. U., "Recovery of deleted records from Microsoft SQL Server log file," Forensic Science and Technology, vol. 31, no. 4, Apr. 2006.
〔6〕 Kim Yeong, "A Study on Forensic Accounting Techniques for Detection of Sign of Fraud Using Financial Statements," M.S. Thesis, Korea University, Aug. 2010.
〔7〕 Ki Min Seo, Jae Min Choi, and Sang Jin Lee, "Design to Forensic Accounting Tool for the Financial Audit," Korea Accounting Information Association, 27(2), pp. 119-144, June. 2009.
〔8〕 Carvey and Harlan, "The Windows Registry as a forensic resource," Digital Investigation, vol. 2, no. 3, pp. 201-205, Sep. 2005.
〔9〕 Singleton, Tommie W., et al. Fraud auditing and forensic accounting, 3rd Ed., John Wiley & Sons, 2006.

〈저 자 소 개〉

이 승 주 (Seung-ju Lee) 학생회원
2016년 2월: 단국대학교 소프트웨어학과 졸업
2016년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 디지털 포렌식

이 국 헌 (Kuk-heon Lee) 학생회원
2012년 2월: 배재대학교 컴퓨터공학 졸업
2014년 8월: 고려대학교 정보보호대학원 석사
2014년 9월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 디지털 포렌식

이 상 진 (Sang-jin Lee) 종신회원
1989년 2월~1999년 2월: 한국전자통신연구원(ETRI) 선임 연구원
1999년 2월~2001년 8월: 고려대학교 자연과학대학 조교수
2001년 9월~현재: 고려대학교 정보보호대학원 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
2015년 1월~2017년 2월: 고려대학교 정보보호대학원 부원장
2017년 3월~현재: 고려대학교 정보보호대학원 원장
〈관심분야〉 디지털 포렌식, 심층 암호, 해쉬 함수