JDFR
Journal of Data Forensics Research
데이터포렌식연구, 1권 1호, 2024년 12월, 1-13면
Journal of Data Forensics Research, Volume 1, Issue 1, December 2024, Pages 1-13.
https://doi.org/10.12972/JDFR.2024.1.1.1
Print ISSN 3058-9460
Online ISSN 3058-9479

원저

데이터포렌식의 개념과 향후 발전방향: 학술적 관점에서

강욱[1], 김지온[2]

[1]경찰대학 행정학과 교수
[2]한림대학교 융합과학수사학과 교수

교신저자: 김지온, jion4ever@gmail.com

요약

본 연구는 데이터 포렌식 및 소셜 네트워크 분석의 개념과 발전 과정을 심층적으로 고찰하며 이들 분야의 중요성을 강조하였다. 한국데이터포렌식학회의 설립을 바탕으로 공공안전과 데이터 사이언스를 융합하는 과정에서 데이터 포렌식의 체계적인 정립이 필요함을 확인하였다. 현재 데이터 포렌식은 범죄 수사와 공공 안전에 필수적인 역할을 하지만, 연구는 여전히 초기 단계에 있으며, 기존 포렌식 분야에 비해 낮은 인식도를 보인다. 이는 명확한 정의와 연구 기반의 부족으로 인해 발생한 문제로, 전문적 접근과 지원이 필요하다는 점을 시사한다. 본 연구는 데이터 포렌식과 소셜 네트워크 분석에서 사용되는 다양한 기법들을 통합적으로 탐구하였으며, 두 분야의 협력이 데이터 수사와 분석의 효율성을 높이는 데 기여할 것이라는 기대를 내포하고 있다. 이러한 연구 결과는 범죄 예방 및 해결, 사이버 보안 강화, 그리고 공공 안전 증진 등 여러 분야에서 데이터 포렌식의 적용 가능성을 넓힐 수 있는 기초가 될 것이다.

결과적으로, 데이터 포렌식의 지속 가능한 발전을 이루기 위해서는 연구, 교육, 그리고 실무에 대한 표준화된 접근 방식이 요구된다. 올바른 정책과 규제를 마련하고, 데이터 포렌식의 중요성을 사회적으로 환기시키는 것이 필요하며, 이를 통해 연구자와 실무자 간의 효과적인 협력 체계를 구축할 수 있을 것이다. 이러한 변화는 데이터 포렌식의 발전을 촉진하고, 다양한 분야에서 책임 있게 활용될 수 있는 기반을 마련할 것이다.

주제어

데이터포렌식, 소셜네트워크 분석, 한국데이터포렌식학회, 표준화, 공공안전

Open Access

Received: November 27, 2024
Revised: December 23, 2024
Accepted: December 24, 2024
Published: December 31, 2024

Original Article

Conceptual Framework and Evolution of Data Forensics: A Scholarly Perspective

Wook Kang[1], Jion Kim[2]

[1]Professor, Department of Public Administration, Korean National Police University, Republic of Korea
[2]Professor, Department of Forensic Science, Hallym University, Republic of Korea

Corresponding Author: Jion Kim, jion4ever@gmail.com

ABSTRACT

This study explores the concepts and development of data forensics and social network analysis, underscoring their importance in contemporary society. It highlights the need for a systematic definition of data forensics, particularly in the context of merging public safety with data science, as exemplified by the establishment of the Korean Data Forensics Society. Although data forensics is crucial for criminal investigations and public safety, it remains less researched and recognized compared to other forensic fields due to a lack of clear definitions and theoretical foundations.

The study integrates various techniques from both data forensics and social network analysis, suggesting that collaboration between these fields can enhance the efficiency of data investigations. These findings advocate for expanding the applications of data forensics in areas such as crime prevention, cybersecurity, and public safety. To ensure sustainable development in data forensics, a standardized framework for research, education, and practice is essential. Implementing appropriate policies and increasing societal recognition of the field's significance will foster better collaboration between researchers and practitioners. These measures aim to advance data forensics and promote its responsible use across various domains.

KEYWORDS

Data Forensics, Social Network Analysis, Korean Data Forensics Society, Standardization, Public Safety

1. 서론

사단법인 한국데이터포렌식학회는 관·산·학·연과 함께 공공안전과 데이터 사이언스를 융합한 학술·연구 인프라 구축, 과학치안 분야를 선도할 데이터 포렌식 생태계를 조성하기 위해 2024년 1월 26일 발족하였다. 연구재단에 포렌식으로 등록되어 있는 학회 및 기관은 8개이며, 포렌식과 관련된 최초의 기관이 2003년에 설립되었다. 포렌식의 오랜 역사와 비교해보면 학문적으로 포렌식이 정립이 되기 시작한 것은 최근의 일이라고 할 수 있다.

일반적으로 포렌식과 디지털포렌식에 대해서는 어느 정도의 연구가 진행이 되고 있는 반면에 데이터포렌식에 대해서는 상대적으로 연구가 미흡한 편이다. 예를 들면, 구글스칼라를 활용하여 “포렌식”을 검색하면 5,540개의 결과물이 탐색되며, “디지털포렌식”으로 검색하면 3,460개의 연구결과를 보여준다. 그러나 “데이터포렌식”으로 검색하면 불과 31개의 연구물이 발견되고 있다. 이를 전세계적으로 확대하면 그 격차는 더욱 벌어진다. “Forensic”은 687,000건, “Digital Forensics”는 82,400건이 검색되나, “Data Forensics”는 2,790건에 불과하다.

일반인의 인식에 영향을 주는 언론기사에 있어서도 많은 차이를 보이고 있다. 뉴스빅데이터 서비스인 BIGKinds를 활용하여 2020년 1월 1일부터 2024년 11월 1일까지의 기사를 검색하였다. 디지털포렌식과 관련된 기사는 15,834건이었으며, 데이터포렌식과 관련된 기사는 1,869건이었다.

데이터포렌식에 대한 연구는 아직 초기 단계에 머물러 있으며, 이 분야는 기존의 포렌식 분야에 비해 상대적으로 주목받지 못하고 있다. 다양한 포렌식 유형, 예를 들어 법의학, 디지털 포렌식 등은 많은 연구와 실무적 응용이 이루어지고 있는 반면, 데이터포렌식은 그 연구량과 응용 사례가 현저히 적다. 이는 데이터포렌식이 무엇인지에 대한 명확한 정의가 부족하고, 관련된 이론 및 실무적 접근 방식이 확립되지 않아서라고 할 수 있다.

본 연구는 데이터포렌식의 개념을 체계적으로 정립하고, 해당 분야의 학문적 발전 방향을 제시하는 것을 주된 목표로 삼고 있다. 이를 위해 우리는 포렌식의 전반적인 개념과 역사, 다양한 종류에 대한 심도 깊은 논의를 진행할 것이다. 포렌식은 범죄 수사와 사건 해결에 중요한 역할을 하며, 과거부터 현재까지의 발전 과정을 추적하여 데이터포렌식이 어떤 맥락에서 발전해왔는지를 살펴볼 것이다.

구체적으로, 포렌식의 기본 원리와 절차, 그에 따른 과학적 접근 방식을 분석하고, 데이터포렌식이 기존의 포렌식 영역에서 발견되는 핵심적인 원칙들과 어떻게 상호작용하는지를 탐구할 것이다. 또한, 다양한 데이터 포렌식 기법과 기술, 실제 사례를 통해 이 분야가 직면하고 있는 도전 과제를 규명하고 해결 방안을 모색할 것이다.

이러한 종합적인 검토를 통해 본 연구는 데이터포렌식의 지속 가능한 발전을 위한 기초를 마련하고, 이 분야의 인식을 제고하여 연구자와 실무자 간의 협력을 촉진할 수 있는 기반을 구축하는 데 기여할 수 있다. 나아가 데이터포렌식이 발전함에 따라, 공공안전, 범죄 예방 및 해결, 그리고 사이버 보안 등 다양한 분야에서의 응용 가능성을 확대할 수 있을 것이다.

2. 포렌식의 의의와 역사

2.1. 포렌식의 개념

‘포렌식’이라는 용어는 라틴어 ‘포렌시스(forēnsis)’에서 유래한 것으로, “포럼의” 또는 “집회 장소와 관련된”이라는 의미를 가지고 있다 [1]. 이 용어의 역사적 뿌리는 고대 로마 사회로

거슬러 올라가며, 당시에는 포럼이 법률 및 시민적 문제를 다루는 데 있어 핵심적인 역할을 지니고 있었다 [2].

로마 시대의 포럼은 시민들이 모여 상업적인 활동뿐만 아니라 법적 문제를 해결하는 중요한 공공 장소였다 [3]. 개인에 대한 형사 고소가 제기되면, 그 사건은 공적인 포럼에서 발표되었으며, 이는 법적 절차의 장으로 기능했다. 이 자리에서 피고인과 고소인은 각각 자신의 입장을 명확히 설명할 수 있는 기회를 가졌고, 많은 시민과 관계자들 앞에서 공개적으로 자신의 주장을 펼쳤다.

이 과정은 본질적으로 적대적인 성격을 띠었으며, 각 당사자의 연설 효과는 사건의 결과에 매우 중요한 역할을 했다. 주장의 강도, 전달의 설득력, 여론을 설득할 수 있는 능력 등 다양한 요소들이 어느 쪽이 승리할지를 결정짓는 데 핵심적으로 작용하였다 [4]. 피고인과 고소인 중에서 누가 가장 설득력 있는 주장을 구성하고, 청중의 관심을 끌며, 증거를 가장 효과적으로 제시했는가에 따라 사건의 결론이 달라지게 되었다.

이러한 역사적 맥락은 오늘날의 “포렌식”이라는 용어의 현대적 의미를 형성하는 데 중요한 영향을 미쳤다. 현재 포렌식은 두 가지 주요 용도로 사용되고 있다. 첫째, 법정에서 인정될 수 있는 법적 증거를 설명하는 용어로서의 기능이 있으며 [5], 둘째, 공개 또는 공식적인 환경에서 정보, 주장, 또는 조사 결과를 발표하는 광범위한 용어로도 사용된다.

따라서 포렌식이라는 용어의 가치와 중요성은 법적 맥락에서 증거와 논증의 이해를 보다 신뢰할 수 있는 형태로 전달하는 커뮤니케이션 및 공개 담론의 역할을 강조한다. 이러한 의미에서 포렌식은 단순히 법률적 의미를 넘어, 사회적, 문화적 차원에서도 중요한 논의의 장으로 확장될 수 있음을 시사한다.

현대 사회에서의 포렌식은 형법과 민법에서 법적 의사 결정 과정을 지원하기 위해 과학적 원리와 방법론을 체계적으로 적용하는 학문적 분야를 의미한다고 할 수 있다[6]. 포렌식은 다양한 과학 분야를 통합하여 사법적 맥락에서 비판적으로 평가될 수 있는 증거를 제공함으로써 사법 행정을 향상시키는 데 기여하고 있다.

특히 범죄 수사에서 포렌식은 증거의 인정 가능성 및 확립된 형사 절차 준수와 관련된 엄격한 법적 기준에 따라 운영된다 [7]. 이는 법정에서 증거가 어떻게 수집되고, 보존되며, 분석되는지가 형사 사건의 결과에 중대한 영향을 미치기 때문이다. 포렌식 분야는 DNA 분석, 지문 검사, 혈흔 패턴 분석, 총기 및 탄도 평가, 독성학, 현미경 검사, 화재 잔해 분석 등 다양한 기술을 활용하는 방대한 영역으로, 각 기술은 사건의 재구성, 범죄자의 식별, 그리고 법적 절차의 지원에 있어서 중요한 역할을 한다.

포렌식 전문가는 수사 과정에서 물리적 증거를 신중하게 수집하고, 보존하며, 분석하는 역할을 맡고 있다. 일부 포렌식 과학자는 범죄 현장에 직접 배치되어 증거를 수집하고, 이러한 증거를 후속 분석을 위해 무결성을 유지하는 방식으로 보존하는 데 중점을 둔다. 반면, 많은 포렌식 전문가들은 실험실 환경에서 작업하면서 법 집행 기관이나 형사 사법 시스템 내의 다른 이해관계자가 제출한 증거에 대한 종합적인 분석을 수행한다.

또한 포렌식 전문가는 금융 범죄 수사를 위해 금융 기록, 은행 거래 또는 기타 정량적 데이터 분석에 중점을 두는 금융 조사 분야를 전문으로 할 수도 있다 [8]. 이러한 전문가는 민간 기업의 컨설턴트로 고용되거나, 학술 연구에 참여하거나, 정부 기관에서 근무함으로써 각기 다른 환경에서 법적 요구를 충족시키기 위한 다양한 서비스를 제공한다.

포렌식 전문가들은 분석 역할 외에도 형사 및 민사 법정에서 전문가 증언을 제공하는 경우가 많다. 이들은 공정한 과학 권위자로서 증언하게 되며, 이러한 역할은 법원의 인식과 사건의 결

과에 상당한 영향을 미칠 수 있다. 검찰 또는 변호인을 대변하여 경험적 증거를 바탕으로 진실을 규명하는 과정을 통해 포렌식의 객관적인 특성이 강조된다.

또한 이론적으로는 모든 과학 분야가 포렌식 조사에 기여할 수 있지만, 포렌식 조사가 요구되는 대부분의 사건을 처리하기 위해 특정 하위 분야들이 발전하였다. 이러한 확립된 분야들은 포렌식의 전문성을 강화하고, 실무에 대한 체계적인 틀을 구축함으로써 높은 수준의 과학적 엄격성과 법적 준수 기반 위에서 조사가 수행될 수 있도록 보장한다. 이러한 노력은 궁극적으로 법적 시스템 내에서 진실과 정의를 실현하는 데 필요한 과학적 지원을 제공하는 데 중점을 두고 있다.

2.2. 포렌식의 발전과정

법의 발전은 정의를 추구하기 위해 법, 과학, 기술이 점점 더 통합되고 있음을 강조한다. 고대에는 표준화된 법의학 관행이 부족하여 신뢰할 수 없는 강제 자백과 목격자의 증언에 의존한 수사로 무고한 사람들을 처벌하거나 범죄자들을 검거하지 못하는 경우가 많았다. 역사적으로, 중국 송나라 시대의 법의학자인 송자(宋慈, 1186-1249)는 최초로 법의학에 대한 연구를 진행하였으며, 그는 살인 사건과 시신 조사를 통해 다양한 시신과 사체를 조사하고 확보한 정보를 기록하여 법의학 체계를 만들었다. 송자는 각 시신을 검수하면서 사망 원인과 과정을 분석하는 방법도 기술하였으며, 그의 저서인 '세원집록(洗寃集錄)'은 법의학의 기초가 되는 중요한 문헌으로 평가받고 있다 [9].

16세기에는 유럽의 의학자들인 암브로이즈 파레와 이탈리아 외과의사 포르투나토 피델리스, 파올로 자키아가 사망 원인을 체계적으로 연구하기 시작하였다. 이들의 연구와 함께 프랑수아 임마누엘 포데레, 요한 피터 프랭크의 저서에서 법의학에 대한 보다 체계적인 접근이 이루어졌다 [10].

18세기는 증거에 기반한 범죄 수사가 논리적이고 과학적인 방법으로 발전하기 시작한 중요한 시기로, 미신과 고문을 대체한 과학적 추론이 강조되었다. 1784년 존 톰스의 유죄 판결은 물리적 증거의 중요성을 보여주는 대표적인 사례로, 이러한 변화를 잘 드러낸다.

법의학이 발전함에 따라 한스 그로스는 과학적 수사 방법을 옹호하며 범죄학의 기초를 마련하였고, 에드몽 로카르는 범죄자가 흔적을 남긴다고 주장하며 교환 원리를 도입하였다 [11]. 20세기 후반에는 혁신적인 발전이 이루어졌으며, 특히 1984년 알렉 제프리스가 유전자 변이를 통해 개인을 식별하는 DNA 프로파일링 기술을 도입하여 범죄 수사에 혁명을 일으켰다 [12].

디지털 포렌식은 1970년대에 디지털 데이터가 급증하면서 주로 메인프레임과 미니컴퓨터를 통해 시작되었다 [13,14]. 1980년대에 개인용 컴퓨터가 널리 보급되면서 컴퓨터 관련 범죄를 조사하는 방법에 대한 필요성이 높아졌고, 초기 포렌식에서는 하드 드라이브에서 데이터를 복구하는 데 중점을 두었다.

1990년대에는 법 집행 기관과 사이버 보안 전문가들이 디지털 범죄 수사를 위한 프로토콜을 공식화하면서 기초적인 기술과 도구가 개발되었다. 1990년대 후반 인터넷의 부상으로 해킹과 신원 도용과 같은 사이버 범죄는 혁신적인 분석 접근법을 필요로 하는 새로운 과제를 안겨주었다. 2000년대 초반에는 디지털 포렌식의 표준화가 진행되었고, IACIS (International Association for Computer Information Systems)와 NIST (National Institute of Standards and Technology)와 같은 기관에서 조사의 일관성을 보장하기 위한 가이드라인을 마련했다 [14]. 2000년대 중반에는 모바일 장치와 디지털 미디어 스토리지가 스마트폰과 USB 드라이브 등 다양한 소스에서 증거를 추출하는 기술을 요구하면서 이 분야가 더욱 확장되었다.

2000년대 후반에는 클라우드 컴퓨팅과 가상화로 인해 복잡성이 증가하며 분산된 스토리지 시스템에서 데이터를 검색하기 위한 적응형 전략이 필요해졌다. 2010년대에는 빅데이터, 머신러닝, 인공지능의 발전이 디지털 포렌식에 큰 영향을 미쳐 패턴 인식을 위한 대규모 데이터 세트의 효율적인 분석이 가능해졌다.

3. 데이터포렌식의 정의와 발전과정

3.1. 데이터포렌식의 개념과 절차

데이터포렌식은 디지털 데이터의 생성, 저장, 활용에 초점을 맞춘 체계적인 조사를 통해 이상 징후를 탐지하거나 범죄에 활용되는 방법으로 정의될 수 있다[15]. 한국데이터포렌식학회 제1회 컨퍼런스(2024. 2. 21.)에서는 '데이터포렌식'이란 공공안전과 형사사법 및 증거조사 분야에서 공공·민간 데이터를 활용하여 범죄나 비정상적인 활동 등을 조사·분석하고, 관련 기술개발과 서비스를 제공함으로써 국민 안전에 기여하는 활동이라고 정의하였다. 디지털 포렌식이 컴퓨터 하드디스크나 스마트폰과 같은 디지털 기기를 대상으로 디지털 증거의 수집과 복구에 초점을 맞추고 있는 반면, 데이터 포렌식은 디지털 기기 뿐만 아니라 온라인 환경에서 수집되거나 통신 및 금융회사에서 제공하는 디지털 정보를 모두 포함하여 정보출처에 제한이 없고, 데이터 수집과 전처리, 비식별화, 분석 및 처리 등 데이터 처리 전반을 아우르고 있어서 그 개념이 점점 확대되어 가고 있다.

포괄적인 분야인 데이터포렌식에는 디지털 증거의 식별, 보존, 복구, 분석 및 제시와 같은 여러 프로세스가 포함된다. 이 분야는 모바일 기기, 컴퓨터, 서버 및 기타 형태의 저장 매체를 포함한 다양한 플랫폼에 적용 가능하다. 또한 전화 통화, 문자 메시지, 이메일과 같은 통신이 네트워크 인프라를 통과할 때 이를 추적하고 분석하는 것까지 확장된다.

데이터 포렌식에서 수집되는 데이터는 일반적으로 영구 데이터와 휘발성 데이터의 두 가지 주요 유형으로 분류할 수 있다[16,17]. 영구 데이터는 저장 장치에 영구적으로 저장된 정보를 의미하며 조사 목적으로 비교적 쉽게 액세스할 수 있다. 반대로 휘발성 데이터는 본질적으로 복구 및 분석이 더 어려운 비영구적이고 일시적인 정보로 구성된다. 후자의 경우 복구 및 분석이 어렵기 때문에 전문적인 도구와 기술이 필요하다.

데이터 포렌식은 일반적으로 수집, 검사, 분석, 보고의 네 가지 필수 단계로 구성된다[18]. 각 단계는 포괄적인 조사를 보장하는 데 중요한 역할을 한다. 수집 단계에서는 무결성을 유지하는 방식으로 디지털 증거를 수집한다. 그 다음에는 데이터를 면밀히 검토하여 잠재적으로 관련성이 있는 정보를 식별하는 조사 단계가 이어진다. 분석 단계에서는 데이터를 면밀히 조사하여 결론을 도출하고 법적 절차를 지원한다. 마지막으로 보고 단계에서는 조사 결과를 명확하고 간결하게 문서화하여 법정이나 기타 법적 상황에서 제시할 수 있다. 이 단계에서는 효과적인 조사를 위해 다양한 기법이 사용된다. 이러한 방법 중 하나는 여러 하드 드라이브에서 확인된 정보를 연결하여 관계와 맥락을 파악하는 교차 드라이브 분석이다. 또 다른 중요한 접근 방식은 실시간 분석으로, 맞춤형 포렌식 도구를 사용하여 컴퓨터의 운영 체제를 실시간으로 검사하고 증거를 추출하는 것이다. 또한 삭제된 파일을 복구하는 것은 일반적으로 숨겨져 있을 수 있는 중요한 증거를 발견하는 데 사용된다.

최근 사회 전분야에서 디지털 혁신이 일어나면서 비즈니스, 마켓팅, 정책, 보건 등 각 분야에서 소셜 빅데이터(Socia Big Data)를 비롯한 디지털 데이터를 분석하는 일련의 과정에서 일종의 데이터 분석 파이프라인(analytics pipeline)을 구축하는 방법론이 주목을 받고 있다[19].

소셜 빅데이터 분석 파이프라인에 따르면 먼저 데이터 관리 단계에서 '데이터 수집-데이터 저장-데이터 전처리-데이터 처리', 데이터 분석 단계에서 '데이터 분석-데이터 해석'의 과정을 거치게 된다[19].

이때 각 단계별로 선결해야 하는 도전적 요소들이 있는데 데이터 관리 측면에서 데이터 수집 시에는 데이터 신뢰성(Data fidelity)·프라이버시(Privacy)·보안(Security)을, 데이터 저장 단계에서는 확장성(Scalability)·가용성(Availability)·무결성(Integrity)을, 데이터 전처리 단계에서는 데이터 품질(Data Quality)을, 데이터 처리 단계에서는 실시간으로 데이터가 처리될 수 있는지 여부인 데이터 스트리밍(Data streaming)과 데이터를 즉시 처리하여 실시간으로 반응하는 실시간 응답(Real-time response) 여부를 해결해야 한다. 다음으로 데이터 분석 관점에서 첫째로 데이터 분석시에는 다양한 형태의 데이터를 일관성있게 분석할 수 있는 문제에 해당하는 이질성(Heterogeneity)을, 데이터 해석 단계에서는 분석결과를 효과적으로 시각화하여 추론 또는 해석하는 데이터 시각화(Data visualization) 방안을 고려해야 한다[19]. 이러한 소셜 빅데이터 분석 파이프라인에 따른 도전요소들은 범죄수사 데이터를 포렌식하는 과정에서도 반드시 고려해야한다.

데이터 포렌식은 디지털 범죄와 사건을 조사하는 데 있어 중추적인 역할을 하며, 다양한 프로세스와 기술을 통합하여 디지털 증거를 발견하고 분석한다. 이 분야에 내재된 구조화된 방법론과 정교한 도구의 활용은 현대 법적 맥락에서 데이터 포렌식의 중요성을 강조하며, 현대 수사에서 없어서는 안 될 요소로 자리 잡았다. 기술이 계속 발전함에 따라 데이터 포렌식에 사용되는 기술과 도구도 계속 발전하여 디지털 범죄로 인한 문제를 해결하고 디지털 증거의 무결성을 유지하는 데 있어 데이터 포렌식 분야가 강력하고 효과적으로 유지될 수 있도록 보장할 것이다.

3.2. 데이터포렌식의 발전과 도전과제

데이터포렌식의 역사는 개인용 컴퓨터가 보급되면서 사이버 범죄가 동시에 증가하던 1980년대로 거슬러 올라간다 [20]. 개인 및 업무 환경에서 컴퓨터가 널리 보급되면서 디지털 증거를 복구하고 조사하기 위한 효과적인 방법론의 필요성이 점점 더 분명해졌다. 데이터포렌식은 디지털 범죄 활동의 문제를 해결하기 위한 전문 분야로 부상하여 수사관이 법적 관점에서 디지털 증거를 분석하고 제시할 수 있게 해준다. 오늘날 데이터 포렌식은 사기, 스파이 활동, 사이버 스토킹, 데이터 절도, 폭력 범죄 등 다양한 범죄를 수사하는 데 필수적인 요소가 되었다 [21]. 데이터 포렌식 증거 표준은 사법 절차에서 물리적 증거와 비교할 수 있도록 설계되었기 때문에 법적 결과를 뒷받침하기 위해서는 디지털 데이터가 진본이고, 인정할 수 있으며, 신뢰할 수 있어야 한다.

데이터포렌식은 그 중요성에도 불구하고 그 효과를 저해할 수 있는 수많은 문제에 직면해 있다. 그 중 대표적인 분야는 기술 영역으로, 실무자들은 다양한 어려움에 직면하게 된다. 주요 기술적 과제에는 데이터에 대한 액세스를 방해할 수 있는 암호화 관련 문제와 효과적으로 조사할 수 있는 데이터의 양을 제한할 수 있는 기기 저장 용량에 따른 제한이 포함된다. 또한, 안티 포렌식 기술이 출현함에 따라 데이터포렌식 조사에 상당한 도전이 되고 있다 [22]. 안티 포렌식은 범죄자들이 포렌식 도구와 방법론을 우회하기 위해 사용하는 다양한 전략을 말하며, 디지털 증거를 은폐하거나 변경하기 위해 설계된 방법론적 접근 방식과 소프트웨어에 대한 개입을 활용한다 [23].

데이터포렌식 조사에는 법적 문제도 많이 발생하여 조사 과정을 복잡하게 만들 수 있다. 트로이 목마와 같은 악성 소프트웨어는 사용자 모르게 유해한 활동을 실행하기 위해 정상 애플리케

이션으로 위장하는 경우가 많기 때문에 소프트웨어의 특성 문제는 특히 주목할 만하다 [24]. 이와 같은 특성으로 인해 개인이 의도적으로 수행한 행위와 손상된 소프트웨어를 통해 실수로 실행한 행위를 구별하기 어렵다. 결과적으로 사이버 범죄 행위의 진정한 의도를 파악하기 쉽지 않다. 이러한 법적 모호성은 사이버 범죄 사건의 기소에 어려움을 초래하고 법정에서 디지털 증거를 효과적으로 사용하는 데 장애가 될 수 있다.

데이터포렌식은 기술 및 법적 문제 외에도 중요한 행정적 문제에 직면하고 있다. 가장 큰 문제는 업계 내 표준화된 관행과 거버넌스가 부족하다는 점이다 [25]. 데이터 포렌식에 대해 인정되는 다양한 표준이 존재하지만, 현재 데이터 포렌식 전문가의 역량과 자격을 규제하는 통일된 프레임워크는 존재하지 않는다. 이러한 표준화의 부재는 실무자마다 다양한 전문성과 방법론적 엄격성을 보유할 수 있기 때문에 실무에서 일관성이 결여되는 결과를 초래한다.

결론적으로, 데이터포렌식의 역사는 개인용 컴퓨터와 휴대폰의 보급, 인터넷의 활용과 함께 진화해 왔으며, 현대 디지털 범죄 수사에서 그 중요성을 입증하고 있다. 그러나 이 분야에서는 데이터 포렌식 수사의 효율성을 저해할 수 있는 다양한 기술적, 법적, 행정적 과제를 해결해야 한다. 표준화된 관행의 개발, 전문가에 대한 교육 강화, 법적 프레임워크의 개선을 통해 이러한 문제를 해결하는 것은 매우 중요하다.

4. 데이터베이스 기반 데이터포렌식과 소셜 네트워크 분석

4.1. 개요

데이터포렌식 분석방법론 중 소셜 네트워크 분석은 수사관들이 수사 정보를 분석하는데 가장 많이 활용되는 분석방법론 중의 하나이다[26]. 왜냐하면 범죄 수사과정에서 수사단서들간의 연관관계를 분석하고 추론 하는 것이 사건의 실마리를 찾는데 큰 도움이 되기 때문이다. 한편 분석대상 수사정보들의 양이 많아지면 한번에 많은양의 데이터를 시각화하여 분석하는 것이 불가능하기 때문에 데이터베이스를 구축하여 필요한 데이터만 추출하여 분석하는 기술이 필요하다. 이 장에서는 데이터포렌식의 주요 방법론인 데이터베이스 기반의 데이터포렌식(이하 '데이터베이스 포렌식'이라고 한다.)과 소셜 네트워크 분석에 한정하여 논의함으로써 데이터포렌식의 주요 두가지 방법론에 대한 구체적인 이해를 높이기로 한다.

소셜 네트워크 분석은 데이터 포렌식 절차 중 '분석'단계에서 하나의 방법론으로 활용이 가능하다. 특히 온라인 소셜 미디어 플랫폼에서 발견되는 비정형 콘텐츠를 조사하는데 많이 활용된다[27]. 데이터베이스 포렌식과 소셜 네트워크 분석 모두 방대한 데이터 세트에서 의미 있는 정보를 추출하는 것을 목표로 하고 있지만, 관련된 데이터의 특성으로 인해 고유한 문제에 직면하고 있다. 데이터베이스 포렌식은 주로 데이터베이스 시스템과 그 콘텐츠의 분석에 중점을 둔 분야이며, 여기에는 데이터 재구성, 메타데이터 분석, 그리고 사고 대응과 같은 핵심 구성 요소가 포함된다. 데이터 재구성은 복잡한 데이터베이스 구조에서 손실되거나 삭제된 데이터를 복구하는 과정이며, 메타데이터 분석은 기본 데이터에 대한 맥락을 제공하는 동반 데이터를 조사하는 작업이다. 사고 대응은 데이터 유출이나 사고 발생 후 증거와 디지털 활동의 흔적을 보존하는 즉각적인 조치를 포함한다.

소셜 네트워크 분석은 디지털 플랫폼에서 개인, 그룹 또는 단체 간의 상호작용과 관계를 조사하는 방법으로, 주로 콘텐츠 분석, 멀티미디어 조사, 및 네트워크 매핑을 통해 이루어진다 [28]. 콘텐츠 분석은 텍스트 데이터(예: 게시물, 댓글)를 조사하여 사용자 정서와 실행 가능한 인사이트를 파악하는 것이며, 멀티미디어 조사는 이미지, 동영상 및 기타 미디어를 평가하여 이벤

트와 장소, 그리고 참여자의 참여도를 파악하는 과정을 포함한다. 마지막으로, 네트워크 매핑은 사용자 간의 관계를 시각화하여 영향력, 커뮤니케이션 또는 부정행위의 패턴을 파악하는 데 기여한다. 이 두 분야의 관계를 이해하는 것은 강력한 조사 전략을 개발하는 데 필수적인 인사이트를 제공한다.

4.2. 데이터베이스 포렌식 및 소셜 네트워크 분석 기법

데이터베이스 포렌식과 소셜 네트워크 분석에서 사용되는 기법들은 각기 다른 데이터의 본질과 분석의 목적에 따라 특별히 개발된 기술들을 포함한다. 이들 기법은 방대한 양의 데이터에서 의미 있는 인사이트를 추출하고, 복잡한 관계를 이해하는 데 필수적이다.

데이터베이스 포렌식의 기법 중 하나는 SQL 기법이다 [29]. SQL(Structured Query Language) 기법은 데이터베이스에서 정보를 검색하고 조작하는 데 사용되는 표준 언어로, 데이터 포렌식에서는 특정 조건을 만족하는 데이터 행위를 찾아내는 데 유용하다. 데이터베이스 시스템에서 발생한 사건의 증거를 수집하고, 특정 조건을 가진 데이터를 추출하기 위해 복잡한 SQL 쿼리를 작성하는 것은 포렌식 팀의 중요한 작업이다. 또한, 데이터베이스의 스키마 인식을 통해 데이터 구조와 관계를 이해하고, 다양한 구성 요소를 탐색하며 데이터를 보다 효과적으로 조작할 수 있다.

메타데이터 분석은 데이터 포렌식에서 또 다른 핵심 기법이다. 메타데이터는 데이터에 대한 데이터를 의미하며, 파일 생성 날짜, 수정 날짜, 작성자 정보를 포함한다 [30,31]. 이러한 메타데이터를 분석함으로써 사건의 타임라인을 재구성하거나, 특정 데이터의 출처를 추적할 수 있다. 예를 들어, 특정 문서의 수정 이력을 통해 누가 언제 어떻게 수정했는지를 확인함으로써 의심스러운 행동을 밝혀내는 데 중요한 역할을 한다. 한국 경찰에서도 대용량 수사정보분석을 할 때 SQL 기반의 관계형 데이터베이스인 i-base를 활용하여 사이버 조직범죄인 보이스피싱 범죄에 대한 대응을 하고 있다[32]. 한국 경찰이 대용량으로 확보하는 대표적인 수사정보가 통화·계좌내역이므로 통신과 금융정보를 위주로 관계형 데이터베이스 스키마를 설계하여 수사정보분석을 진행하고 있다.

주로 디지털 포렌식에 해당하는 사고 대응 기법도 중요하다. 사건 발생 시 신속하게 데이터를 수집하고 분석하는 절차는 포렌식 조사에서 필수적이다. 이러한 과정에서는 증거를 보존하고, 데이터가 변경되거나 삭제되는 것을 방지하기 위해 이미지 복사본을 생성하고, 원본 데이터와의 무결성을 보장해야 한다. 이 과정에서 포렌식 소프트웨어 도구가 사용되며, 이는 데이터 복구 및 분석을 지원하는 다양한 기능을 제공한다.

소셜 네트워크 분석에서는 다양한 기법이 활용된다. 그중 하나는 그래프 이론에 근거한 네트워크 분석 기법이다. 그래프 이론을 통해 사용자 간의 관계를 모델링하고, 이를 시각화함으로써 특정 전파 패턴, 커뮤니케이션 흐름, 영향의 구조를 파악할 수 있다 [33]. 네트워크의 중심을 이해하면, 영향력 있는 사용자를 식별하거나, 숨겨진 커뮤니티를 발견하는 데 도움이 된다. 소셜 네트워크 분석 모듈 중에서 특히 중심성(centrality)과 하위집단(cohesive subgroup)을 식별하는 원리는 배후에 숨겨진 중요범죄자나 공범집단을 특정하는 등 다양한 목적으로 수사정보분석에 활용되고 있다[34]. 최근에는 범죄혐의의 증명력을 제고하기 위한 방법으로 등위성(equivalence) 원리를 활용하거나[26] 사이버금융범죄에서 범행에 사용된 제3의 계좌나 메신저 계정을 추적하기 위해 2-모드 분석이 활용되기도 하였다[35].

콘텐츠 분석 역시 소셜 네트워크 분석의 중요한 부분이다. 여기에서는 자연어 처리(NLP) 기술을 활용하여 텍스트 데이터를 분석하는데, 이는 게시물이나 댓글에서 의견과 감정을 추출하

는 데 도움을 준다 [36]. 예를 들어, 특정 주제에 대한 대중의 감정이 긍정적인지 부정적인지를 판단하는 데 사용할 수 있다. 감정 분석은 특정 사건이나 이슈에 대한 사회적 반응을 이해하는 데 중요한 기법이다. 최근에는 챗지피티(ChatGPT)와 같은 LLM을 기술을 활용하여 비정형 데이터에서 별도의 데이터 전처리 과정을 거치지 않고 노드(node)와 링크(link)의 속성 정보를 바로 추출하여 시각화 한 후 분석하는 연구도 진행되고 있다[37].

멀티미디어 조사 또한 소셜 네트워크 분석에서 중요한 역할을 한다. 이미지와 비디오 콘텐츠를 평가하여 사건의 전개를 시각적으로 재구성하는 과정이 포함된다. 딥러닝 기술, 특히 컨볼루션 신경망(CNN)을 사용하여 이미지에서 객체를 식별하거나, 비디오에서 특정 행동을 감지하는 등의 작업이 가능하다 [38]. 예를 들어, 범죄 사건의 비디오를 분석하여 피의자를 식별하는 데 기여할 수 있다.

머신 러닝 기법은 데이터 포렌식과 소셜 네트워크 분석 모두에 혁신적인 변화를 가져왔다. 데이터베이스 포렌식에서는 정상적인 트랜잭션 패턴을 학습시킨 후, 이를 기반으로 비정상적인 거래를 탐지하는 시스템이 구축된다. 머신 러닝 알고리즘은 대량의 데이터를 통해 스스로 학습하고 적응할 수 있어, 조사자가 의심할 만한 활동을 신속하게 감지할 수 있도록 돕는다 [39]. 소셜 네트워크 분석에서도 머신 러닝은 비정상적인 상호작용을 탐지하여 허위 정보 캠페인이나 자동화된 봇 계정을 식별하는 데 중요한 역할을 한다.

이러한 기법들은 개별적으로 사용될 수도 있지만, 함께 통합되어 강력하고 포괄적인 분석 능력을 제공한다. 데이터 포렌식과 소셜 네트워크 분석 기법이 상호 보완적으로 작용함으로써, 더욱 정교하고 신뢰할 수 있는 결과를 도출할 수 있다.

4.3. 데이터베이스 포렌식 및 소셜 네트워크 분석의 과제

데이터베이스 포렌식과 소셜 네트워크 분석은 각각 고유한 도전 과제를 안고 있다. 데이터베이스 포렌식의 경우, 데이터가 수정되거나 삭제될 수 있으므로 빠른 액세스와 분석이 필수적이다. 이러한 변동성은 데이터를 효율적으로 수집하고 유지하는 데 어려움을 초래한다 [40].

소셜 네트워크 분석에서는 특히 온라인 데이터를 활용할 때 소셜 미디어 콘텐츠의 일시적인 특성과 사용자의 게시물에 대한 통제권이 문제된다. 사용자는 언제든지 게시물을 변경하거나 삭제할 수 있으며, 이로 인해 데이터 수집과 분석이 복잡해진다 [41]. 게시물이 문맥을 잃거나 삭제되면 중요한 증거를 놓칠 수 있다.

데이터의 양과 다양성 또한 도전 과제다. 데이터베이스 포렌식에서는 전통적으로 구조화된 데이터베이스가 방대한 데이터 유형을 포함할 수 있으며, 이는 다양한 구조와 형식을 처리하기 위한 전문화된 도구를 필요로 한다. 반면, 소셜 네트워크 분석은 생성되는 콘텐츠의 양이 방대하여 데이터를 정확하게 처리하고 필터링하는 데 어려움이 있다. 텍스트, 이미지, 동영상 등 다양한 형식의 콘텐츠는 적응 가능하고 확장 가능한 분석 프레임워크를 요구한다.

두 분야 모두 개인의 고유한 특성이나 패턴에 해당하는 시그니처(signature)나 행동을 추적해야 하는 도전에 직면해 있다. 온라인 상호작용의 익명성은 콘텐츠의 신뢰성과 사용자의 신원에 관한 중대한 의문을 제기한다. 이러한 맥락에서 디지털 풋프린트(foot-print) 분석을 통해 플랫폼에 남겨진 흔적을 활용하여 행동이나 신원을 연결하는 기술이 필요하지만, 이는 여전히 복잡한 과제다. 관계 매핑을 통해 숨겨진 관계를 밝혀내는 것은 모호하거나 익명의 계정에 대한 이해를 돕는 데 기여할 수 있지만, 신뢰성이 담보되지 않은 데이터의 신원을 추적하는 일은 쉽지 않다.

또한, 데이터베이스 포렌식과 소셜 네트워크 분석은 사용자 개인정보와 관련된 윤리적 딜레

마에 빠질 수 있다. 데이터 수집과 분석이 개인의 프라이버시를 위협할 수 있으며, 부당한 감시나 침입적인 데이터 수집에 대한 반발이 커지고 있다. 따라서 법적 및 윤리적 기준을 철저히 준수해야 하며, 이러한 기준을 준수하기 위한 구체적이고 실용적인 조치가 필요하다.

이처럼 데이터베이스 포렌식과 소셜 네트워크 분석 각각은 여러 도전 과제에 직면해 있으며, 이들 두 분야에서 협력하여 이러한 문제를 해결하는 것이 중요하다. 디지털 환경이 변화함에 따라 이러한 도전과제를 극복하기 위한 혁신적이고 통합적인 접근 방식이 필요하다.

5. 결론

사단법인 한국데이터포렌식학회는 공공안전과 데이터 사이언스를 융합한 학술·연구 인프라 구축을 목표로 하고 있으며, 이를 통해 과학치안 분야를 선도할 데이터 포렌식 생태계를 조성하고자 2024년 1월 26일 발족하였다. 여러 통계들을 살펴보면 데이터 포렌식에 대한 연구가 아직 초기 단계에 머물러 있으며, 기존의 포렌식 분야에 비해 상대적으로 낮은 주목을 받고 있다는 것을 분명하게 드러낸다. 다양한 포렌식 유형, 예를 들어 법의학이나 디지털 포렌식은 많은 연구와 실무적 응용이 이루어지고 있는 반면, 데이터 포렌식은 그 연구량과 응용 사례가 현저히 적다는 사실이 주목할 만하다.

따라서 본 연구는 데이터 포렌식의 개념을 체계적으로 정립하고, 이 분야의 학문적 발전 방향을 제시하는 것을 주된 목표로 하고 있다. 연구를 통해 포렌식의 전반적인 개념과 역사, 그리고 다양한 유형에 대한 심도 있는 논의를 진행하였으며, 데이터 포렌식이 과거부터 현재까지 어떤 맥락에서 발전해왔는지를 분석하였다.

특히, 본 연구는 데이터베이스 포렌식 및 소셜 네트워크 분석의 개념과 발전 과정을 심층적으로 고찰하며, 이들 분야의 중요성과 기여와 최근 트렌드를 명확히 하였다. 데이터 포렌식은 빠르게 변화하는 디지털 환경 속에서 범죄 수사 및 공공안전에 필수적인 역할을 수행하고 있으며, 이 분야의 연구는 기술 발전과 사회적 필요에 따른 새로운 도전과제를 해결하는 데 중점을 두어야 할 것이다.

아울러 데이터 포렌식은 다양한 데이터 유형과 형식의 출현으로 인해 복잡한 상황을 다루어야 하며, 기존 포렌식의 경험을 바탕으로 더욱 진화해 나가야 한다. 그러나 현재 데이터 포렌식에 대한 연구는 상대적으로 초기 단계에 있으며, 구체적인 정의와 이론적 기반의 부족으로 인해 연구량이 미비한 상태임을 확인하였다. 이는 데이터 포렌식이 과거의 전통적인 포렌식 분야와 비교할 때 자리를 잡아가는 과정에 있으며, 이에 대한 체계적인 접근이 필요하다는 점을 시사한다.

더 나아가 본 연구는 데이터베이스 포렌식과 소셜 네트워크 분석에서 사용되는 기법들을 통합적으로 탐구하며, 두 분야의 협력이 데이터 수사와 분석의 효율성을 높이는 데 기여할 것이라는 전망을 제시하였다. 두 분야는 상호 보완적인 특성을 지니고 있어, 함께 발전함으로써 범죄 예방 및 해결, 사이버 보안 강화, 공공 안전 증진의 이점을 가져올 수 있다.

결론적으로, 데이터 포렌식의 지속 가능한 발전을 이루기 위해서는 해당 분야의 연구와 교육, 그리고 실무에 대한 표준화된 접근 방식이 요청된다. 올바른 정책과 규제를 마련하고, 데이터 포렌식의 중요성을 사회적으로 환기시킴으로써 연구자와 실무자 간의 효과적인 협력 체계가 구축될 것으로 기대된다. 이러한 변화는 데이터 포렌식 생태계가 더욱 발전하고, 다양한 분야에서 책임 있는 방식으로 활용될 수 있는 기반이 될 것이다.

참고문헌(References)

[1] Foster Jacob. 2023. The “autopsy” enigma: etymology, related terms and unambiguous alternatives. Forensic Science, Medicine and Pathology, 20, 1491-1498.

[2] Porta D. 2005. Making the polis: social forums and democracy in the global justice movement. Mobilization: An International Quarterly, 10, 73-94.

[3] Russell A. 2016. The politics of public space in Republican Rome, pp. 77-79. Cambridge University Press.

[4] Landsman S. 1983. A Brief Survey on the Development of the Adversary System.Ohio State Law Journal, 44, 713.

[5] Jung JH, Lee CM. 2017. A Study on Integr ity, Originality, and Reliability of Digital Forensic based on Comparison of Standard Guidelines and precedents. Journal of Digital Forensics , 11(3), 41-55.

[6] Franjić Siniša. 2018. Legal aspects of Forensics. Forensic Science Today, 4(1),9-17.

[7] Baek SJ, Shim MN, Lim JI. 2008. National digital forensics legal frameworks and the state of digital forensics legislation at home and abroad (국가 디지털 포렌식 법률 체계와 국내외 디지털 포렌식 법제 현황). Review of KIISC, 18(1), 49-61.

[8] Odeyemi O, Ibeh CV, Mhlongo NJ, et al. 2024. Forensic accounting and fraud detection: a review of techniques in the digital age. Finance & Accounting Research Journal, 6(2), 202-214.

[9] Kwak JS. 2006. A Review of Postmortem Investigation of Joseon Dynasty in the Aspect of Recent Forensic Medicine. Journal of Forensic and Investigative Science 1(1), 5-10.

[10] Lindberg DC, Park K, Porter R, et al. 2003. The Cambridge History of Science: Volume 3, Early Modern Science, pp. 316-317. Cambridge University Press.

[11] Kim EK, Jo HB. 2016. Reinterpretation of Heumheum Sinseo as Investigation and Forensic Manual. The Journal of the Korea Contents Association, 16(5), 583-590. https://doi.org/10.5392/JKCA.2016.16.05.583

[12] McDonald J, Lehman DC. 2012. Forensic DNA analysis. Clinical Laboratory Science, 25(2), 109-113.

[13] Ahn MT, Kwon HY. 2022. Implementation of the right to control personal information by guaranteeing the right to participate in the search and seizure of digital evidence. Journal of Digital Forensics, 16(3), 88-101.

[14] Jones GM, Winster SG. 2022. An insight into digital forensics: history, frameworks, types and tools. Cyber Security and Digital Forensics (2022): 105-125. https://doi.org/10.1002/9781119795667.ch6

[15] de Klerk S, van Noord S, van Ommering C. 2019. The Theory and Practice of Educational Data Forensics. In: Veldkamp B, Sluijter C, editors. Theoretical and Practical Advances in Computer-based Educational Measurement. Methodology of Educational Measurement and Assessment. Springer, Cham. https://doi.org/10.1007/978-3-030-18480-3_20

[16] Lee E, Park D. 2023. Performance Analysis of Real-Time Big Data Search Platform Based on High-Capacity Persistent Memory. Journal of Platform Technology, 11(4), 50-61.

[17] Mann HK, Chhabra GS. 2016. Volatile memory forensics: a legal perspective. International Journal of Computer Applications, 155(3), 11-15. https://doi.org/10.5120/ijca2016912276

[18] Nasreldin MM, El-Hennawy M, Aslan HK, et al. 2015. Digital forensics evidence acquisition and chain of custody in cloud computing. IJCSI International Journal of Computer Science Issues, 12(1), 153-160.

[19] Sebei H, Taieb MAH, Aouicha MB. 2018. Review of social media analytics process and Big Data pipeline. Social Network Analysis and Mining, 8, 30. https://doi.org/10.1007/s13278-018-0507-0

[20] Horsman G. 2017. Can we continue to effectively police digital crime?. Science & Justice, 57(6), 448-454. https://doi.org/10.1016/j.scijus.2017.06.001

[21] Mishra P. 2020. Big data digital forensic and cybersecurity. In: Big Data Analytics and Computing for Digital Forensic Investigations, pp. 183-203. CRC Press.

[22] Shin W. 2014. Countermeasures against Anti-forensics by Analyzing Anti-forensics Techniques. Journal of Security Engineering, 11(6), 605-614.

[23] Park G, Hong S, Kim J, et al. 2016. A Study on Comparison Analysis of Digital Forensic Technology for Preventing Information Leakage. Convergence Security Journal, 16(7), 93-100.

[24] Chang YJ, Cha MS, Jung JS, et al. 2008. Malware trends and their future outlook (악성 코드 동향과 그 미래 전망). Review of KIISC, 18(3), 1-16.

[25] Vincze EA. 2016. Challenges in digital forensics. Police Practice and Research, 17(2), 183-194.

[26] Kim JO, Woo B. 2022. A Study on Cybercrime Detection and Analysis Technology. Journal of Korean Public Police and Security Studies, 19(3), 57-76.

[27] Chopade R, Pachghare V. 2019. Ten years of critical review on database forensics research. Digital Investigation, 29, 180-197. https://doi.org/10.1016/j.diin.2019.04.001

[28] Camacho D, Panizo-LLedot Á, Bello-Orgaz G, et al. 2020. The four dimensions of social network analysis: An overview of research methods, applications, and software tools. Information Fusion, 63, 88-120.

[29] Seo Y, Park S. 2017. HTTP Request - SQL Query Mapping Scheme for Malicious SQL Query Detection in Multitier Web Applications. Journal of KIISE, 44(1), 1-12. https://doi.org/10.5626/JOK.2017.44.1.1

[30] Yoo S. 2010. A Diagnostic Analysis of Metadata R&D Status in Korea. Journal of the Korean Society for Library and Information Science, 44(2), 405-426.

[31] Harrison F. 2011. Getting started with meta-analysis. Methods in Ecology and Evolution, 2(1), 1-10.

[32] Kim KJ. 2022. Big Data Analytics for Tracking Evolving Digital Voice Phishing Crimes and Preventing Money Laundering. Anti-Money Laundering and Financial Fraud Conference(진화하는 디지털 보이스피싱 범죄 추적 및 자금세탁 방지를 위한 빅데이터 분석 발제문, 경찰대학 자금세탁·금융사기 방지 학술컨퍼런스). Korean National Police University, 2022. 4. 27.

[33] Kolomeets M, Chechulin A, Kotenko I. 2019. Social networks analysis by graph algorithms on the example of the VKontakte social network. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 10(2), 55-75.

[34] Kim JO. 2019. A Study on the Application of Social Network Analysis Principles to Criminal Investigation. Journal of Digital Forensics, 13(2), 87-107.

[35] Kim HC, Yoon JW. 2020. A Case of Cyber Financial Crime Investigation Through Social Network Analysis (2-Mode Concepts). Journal of Digital Forensics, 14(4), 449-465.

[36] Bokolo BG, Liu Q. 2024. Artificial Intelligence in Social Media Forensics: A Comprehensive Survey and Analysis. Electronics, 13(9), 1671.

[37] Kim JO. 2024. Integrated Analysis of Cyber Organized Crime. The 2nd Academic Conference of the Korean Data Forensics Society, 2024. 7. 11.

[38] Lee JW. 2017. A study on an efficient hand gesture recognition method using 3D-CNN (3D-CNN을 이용한 효율적인 손 제스처 인식 방법에 관한 연구). PhD dissertation. Seoul National University, Seoul, Korea.

[39] Chkirbene Z, Erbad A, Hamila R, et al. 2020. Machine learning based cloud computing anomalies detection. IEEE Network, 34(6), 178-183.

[40] Park K, Kusiak A. 2005. Enterprise resource planning (ERP) operations support system for maintaining process integration. International Journal of Production Research, 43(19), 3959-3982. https://doi.org/10.1080/00207540500140799

[41] Zhao X, Lampe C, Ellison NB. 2016. The social media ecology: User perceptions, strategies and challenges. Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, pp. 89-100.