데이터베이스 포렌식 기술 및 산업(연구) 동향

컴퓨터공학과
20180976 김혜인

1. 데이터베이스 포렌식과 디지털 포렌식

포렌식은 증거를 수집하고 보존하여 처리하는 과정에서 법정에서 증거로 활용할 수 있도록 과학적, 기술적인 기법을 사용하되 증거의 가치가 상실되지 않도록 하는 일련의 절차를 의미한다. 디지털 포렌식은 전자적 증거물 등을 사법기관에서 사용할 수 있도록 데이터를 수집, 분석하는 일련의 과정을 말한다.

데이터베이스 포렌식이란 데이터베이스에서 데이터를 추출, 분석하여 증거를 획득하는 포렌식 분야로 디지털 포렌식의 하나의 유형이다. 따라서 데이터베이스 포렌식 기술 및 산업의 동향을 살펴보기 위해서는 디지털 포렌식의 동향을 살펴보는 것이 우선 되어야 한다.

2. 디지털 포렌식 동향

디지털 포렌식은 약 40년 정도의 역사를 가진다. 1970년대 후반~1980년대 초반, 미국을 중심으로 저작권, 개인 정보 보호, 사이버 스토킹, 아동 포르노와 같은 문제들이 생겨나면서 컴퓨터 관련 범죄 관련 법이 만들어지기 시작했다. 이러한 컴퓨터 범죄의 증가로 이에 대처하기 위한 과학수사와 조사 기술, 증거 수집 기술이 필요하게 되면서 디지털 포렌식이 생겨났다. 초창기에는 컴퓨터를 중심으로 한 컴퓨터 포렌식이 생겨났으나, 점차 증거를 포함하고 있는 분석대상이 컴퓨터에서 다양한 디지털 장비로 확대되며 컴퓨터 포렌식에서 디지털 포렌식으로 변화하게 되었다.

이후 2000년대까지 디지털 포렌식의 황금기라 불릴 정도로 다양한 방면에서 디지털 포렌식의 발전이 이루어졌다. 디지털 포렌식 관련 기관들이 설립되고, 국가별 디지털 포렌식 표준이 수립되는 등 국가기관을 중심으로 디지털 포렌식 정책 및 기술 연구, 법 제정들이 꾸준히 이루어졌다. 또한 컴퓨터 및 모바일 기기, 인터넷 등 IT 기술의 발전이 지금만큼 이뤄지지 않았던 2000년대에는 저장 장치의 용량이 작고, 용의자가 소유한 한 대의 컴퓨터만을 대상으로 분석을 진행하는 경우가 많았기 때문에 디지털 포렌식이 더욱 쉽게 이뤄질 수 있었다. 이러한 배경을 바탕으로 하나의 기기에 대한 포렌식 기술 연구를 더욱 집중적으로 할 수 있고, 전용 도구들을 개발하여 더욱 디지털 포렉식에 쉽게 접근할 수 있었다.

하지만 2010년대에 접어들면서 디지털 포렌식이 위기에 빠지게 된다. 저장 장치의 용량이 크게 증가하고, 모바일 기기, 운영 체제, 파일 포맷 등이 증가하면서 데이터 분석이 어려워지고, 웹 기술의 발전으로 클라우드 컴퓨팅 등이 생겨나면서 증거 데이터 수집이 어려워진다. 또한 암호화와 같은 안티 포렌식 기술이 발전하면서 디지털 포렌식이 더욱 난항을 겪게 된다. 디지털 포렌식 대상이 늘어나면서 디지털 포렌식이 디스크 포렌식, 시스템 포렌식, 데이터베이스 포렌식, 모바일 포렌식 등으로 세분화 되고, 기존 디지털 포렌식 도구들의 한계가 드러나게 되면서 디지털 포렌식은 많은 연구 과제를 안게 된다. 또한 디지털 포렌식 관련 법/제도 등이 마련되면서 오히려 디

지털 포렌식 기술의 적용 범위가 제한되면서 디지털 포렌식 접근이 어려워지게 된 문제도 생겼다.

이처럼 디지털 포렌식의 전반적인 흐름을 살펴보면 국내 디지털 포렌식의 기술 및 연구 동향 또한 파악할 수 있다. 디지털 포렌식이 본격적으로 연구된 2000년대부터 살펴보면 초창기에는 디지털 포렌식 국내 도입을 위한 법적 문제나, 디지털 포렌식 모델, 수집 절차 및 무결성 입증을 위한 연구들이 많이 이루어졌음을 예상할 수 있다. 또한 윈도우 운영체제가 설치된 데스크탑이 주된 분석 대상이었던 당시에는 윈도우 시스템에 대한 디지털 포렌식 연구 및 분석 도구들의 연구가 활발했음을 예상할 수 있다. 이후 다양한 운영 체제 및 모바일 기기, iot 기기 등 분석 대상이 늘어나면서 이에 관한 연구들이 생겨나고, 안티 포렌식 기법을 해결하기 위한 연구, 웹의 발달로 인한 다양한 웹 어플리케이션, 클라우드 포렌식을 위한 연구 등 새로운 기술이나 기법의 등장에 따른 연구들이 나타났음을 예상할 수 있다.

따라서 이후 디지털 포렌식의 발전 동향 역시 새로운 기술이 나타남에 따라 계속해서 연구들이 진행될 것임을 예상할 수 있고, 디지털 포렌식의 방법론에 관한 연구와 법적 연구가 동시에 진행되며, 이에 따라 확립된 디지털 포렌식 절차에 따라 다양한 기기나 시스템, 프로그램들에 디지털 포렌식이 적용될 것이라 예상된다.

3. 데이터베이스 포렌식 동향

데이터베이스 포렌식은 데이터베이스의 구조 및 저장된 데이터, 메타데이터를 수집하여 법적 증거 자료로서의 요구 조건을 충족시키기 위해 분석하는 행위이다. 디지털 포렌식의 한 분야로, 데이터베이스 시스템 사용이 늘어나고 이에 따라 데이터베이스를 다루는 디지털 포렌식의 필요성이 대두하면서 생기게 되었다.

데이터베이스 포렌식은 디지털 포렌식의 개념이 어느 정도 확립된 이후에 나타났으므로, 데이터베이스가 가진 특성과 여러 데이터베이스 종류, 관리 시스템에 따른 연구들이 집중적으로 진행되었다.

데이터베이스의 종류로는 크게 관계형 데이터베이스와 NoSQL 데이터베이스가 있다. 관계형 데이터베이스는 행, 열로 구성된 테이블 간의 관계로 데이터들을 표현한 데이터베이스로, SQL이라 불리는 질의문을 통해 데이터를 관리 및 접근할 수 있다. NoSQL 데이터베이스는 최근 많이 사용되는 데이터베이스로 키와 값 형태로 데이터를 저장하여, 키를 사용해 데이터 관리 및 접근을 한다.

컴퓨터의 보급과 함께 데이터베이스 관리 시스템을 사용하여 데이터베이스가 제대로 사용되기 시작한 1990년대 말부터 지금까지 관계형 데이터베이스 관리시스템(RDBMS)이 데이터베이스 시장을 장악하고 있다. 하지만 2000년대 중반 이후 SNS 서비스가 급속도로 발전하고, 빅데이터와 같은 개념이 생기면서 복잡한 관계형 데이터베이스를 해결한 NoSQL에 대한 연구가 많이 이뤄지고 있다. 이에 따라 NoSQL 데이터베이스 시스템도 많이 생겨나고 있다.

데이터베이스에 대한 위와 같은 배경을 바탕으로 데이터베이스 포렌식 기술 및 연구 동향을 살펴보면 2000년대에는 주로 관계형 데이터베이스 시스템(RDBMS)의 전반적인 데이터베이스 포렌식 연구와 함께 RDBMS 중 가장 많은 시장 점유율을 가진 Oracle, MySQL 데이터베이스의 데이터베이스 포렌식이 연구되었음을 알 수 있다. 이후 2010년대에 들어오면서 모바일 기기의 보급이 늘어나면서 안드로이드 폰에서 사용하는 데이터베이스 SQLite에 대한 데이터베이스 포렌식에 관한 연구가 이뤄졌음을 알 수 있고, SNS, 인공지능 등의 발전으로 인해 데이터를 대용량으로 관리하는 빅데이터의 필요성이 생기자 NoSQL에 대한 연구와 함께 MongDB와 같은 데이터베이스 관리 시스템이 생겨나고 이에 따라 MongDB에 대한 데이터베이스 포렌식 연구들이 이뤄지게 됐음을 알 수 있다.

따라서 데이터베이스 포렌식의 발전 동향은 데이터베이스가 빅데이터, NoSQL, 클라우드, 오픈소스 등의 이슈에 따라 크게 변화하고 있음에 따라 많은 변화가 있을 것으로 예상한다. 또한 NoSQL과 클라우드에 대한 관심도가 올라간 지 오래되지 않아 최근까지는 MongoDB, Redis와 같은 NoSQL 데이터베이스 관리 시스템과 클라우드 포렌식에 관한 연구가 집중될 것으로 예상한다.

4. 참고문헌

- 곽나연,이중정,맹윤호,조방호,이상은. "메타스터디를 통한 국내 디지털 포렌식 연구 동향." 정보화정책 24.3 (2017): 91-107.
- 이상진. “디지털포렌식 기술동향 및 발전전망.” IT 산업전망 컨퍼런스