디지털 증거능력 확보 강화를 위한 디지털 포렌식 연구동향 메타분석

류 보 라* · 전 민 서** · 지 주 연*** · 이 찬 우**** · 장 항 배*****

요 약

최근 정보통신기술의 발전에 따라 디지털 정보를 포함한 다양한 데이터들이 기하급수적으로 증가하였으며 이러한 데이터의 활용이 보편화된 최근의 사회는 수사와 재판과정에도 많은 변화를 주었다. 하지만 기하급수적으로 늘어나고 있는 디지털 증거에 대한 기술력과 분석력의 진보에 비해 디지털 포렌식 관련 법과 제도의 확립은 아직 부족한 실정이다. 그러므로 디지털 증거의 법적인정을 위해서는 균형 잡힌 연구의 활성화가 필요하다. 따라서 본 연구에서는 디지털 포렌식 관련 연구동향을 파악하고, 연구 활성화를 위한 객관적 데이터를 제공하기 위하여 메타분석을 진행하였다.

Meta Analysis on Digital Forensics Research Trends for Securing its Admissibility of Digital Evidence

Bora Ryu* · Minseo Jeon** · Juyeon Ji*** · Chanwoo Lee**** · Hangbae Chang*****

ABSTRACT

With the development of information and communication technology, various data including digital data have increased exponentially. In a society where such data utilization is generalized, criminal investigation processes and trial processes have also been influenced. However, in comparison with the progress of the technical capability and analytical capability of digital certification which is increasing exponentially, the establishment of the digital forensic related legal system is still in short supply. Therefore, it is necessary to activate balanced research for legal recognition of digital certification. Therefore, in this research, meta analysis was conducted to grasp trends of research related to digital forensics and to provide objective data for research revitalization.

Key words : 디지털 증거, 디지털 포렌식, 산업보안, 메타분석, 연구동향

접수일(2017년 5월 27일), 게재확정일(2017년 6월 26일)

★ 본 논문은 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음. (IITP-2017-2014-0-00636)

* (주)더존비즈온 포렌식센터

, * 중앙대학교/일반대학원 산업융합보안학과

**** 중앙대학교/일반대학원 융합보안학과

***** 중앙대학교/경영경제대학 산업보안학과(교신저자)

1. 서 론

정보통신기술이 발전함에 따라 사람들이 일상생활에서 디지털 환경을 접하고 디지털 정보를 활용하고 있으며, 다양한 데이터가 빠른 속도로 축적되고 있다. 이러한 최근의 디지털 사회의 변화는 검찰수사와 재판과정에도 많은 변화를 주었다. 경찰청의 산업기술유출사건 검거실적 발표에 따르면 디지털 자료를 이용하여 산업기술을 유출한 경우가 약 80%에 달하고 있는 것으로 나타났다. 사물인터넷과 모바일 기술을 통해 디지털 정보를 활용할 수 있는 다양한 디지털 기기가 개발되고 연결됨에 따라 최근의 범죄행위는 디지털 기기를 활용한 경우가 많아진 것으로 나타났으며 수사를 위하여 제출하는 증거는 대부분 디지털 증거형태로 제출되고 있어, 디지털 증거의 중요성이 갈수록 높아지고 있다. 디지털 포렌식의 필수 불가결한 요소는 바로 과학적이고 합법적인 절차이다. 이러한 절차를 거쳐 만들어진 증거는 수사 관점에서의 디지털 포렌식의 쟁점이라고 할 수 있는 '증거능력'을 갖추게 되기 때문이다. 물론 디지털 포렌식 기술이나 분석도 매우 중요하지만 증거능력을 갖추지 못하면 기술력이나 분석력이 아무리 뛰어날지라도 그 증거는 아무런 효력을 가질 수 없다. 더욱이 기하급수적으로 늘어나고 있는 디지털 증거에 대한 기술력과 분석력의 진보에 비해 디지털 포렌식 관련 법과 제도의 확립은 아직 부족한 실정이다. 그러므로 디지털 증거의 법적 인정을 위해서는 연구의 활성화가 필요하다. 단순히 연구의 물리적인 양에 대한 활성화가 아닌, 상대적으로 발전되어있는 연구영역은 무엇인지, 또한 반대로 연구가 빈약한 영역은 무엇인지 파악하여야 한다. 나아가 한 영역에 치우치지 않은 디지털 포렌식 전 영역에 걸친 균형 있는 연구의 발전이 요구되는 실정이다.

2. 선행연구

2.1 디지털 포렌식

디지털 포렌식은 "사건에 사용된 디지털 자료를 법정에서 증거로 활용하기 위해 증거를 확보하는 기술 및 방법을 연구하는 분야"로 정의된다. 그러므로 디지털 포렌식은 일반적으로 컴퓨터 관련사건 수사를 지원하며, 각종 디지털 자료가 법적인 효력을 가질 수 있도록 과학적·논리적 절차와 방법을 연구하는 기술인 것이다[1]. 디지털 포렌식은 디지털 매체에 저장된 디지털 자료를 근거로 삼아 그 디지털 매체로 하여 일어난 어떤 행위에 대한 사실관계를 규명하고 증명하는 기법이다. 다양한 디지털 매체의 활용도가 높은 현 시대에서 이를 악용하는 범죄가 기하급수적으로 늘어나면서 디지털 매체에 저장되어 있는 자료가 법정에서 다루어지는 경우가 매우 많다. 디지털 매체에 저장된 자료는 일반적으로 복사가 쉬울 뿐만 아니라 원본과 복사본의 구분이 어렵고 조작 및 생성, 전송, 삭제가 매우 용이하다. 따라서 디지털 자료가 증거능력을 갖추기 위해서는 자료의 수집·보존·분석·보고에 이르는 전 과정에 특별한 절차와 방법이 따라주어야 한다. 이렇게 디지털 자료가 증거능력을 갖도록 하는 절차와 방법을 디지털 포렌식이라고 한다[1]. 그러므로 디지털 포렌식은 단순히 과학적인 수사방법이자 절차일 뿐 아니라 법률, 제도 그리고 각종 기술 등을 포함하는 종합적인 분야라고 할 수 있다.

2.2 디지털 증거

디지털 증거는 전자적 증거, 전파기록, 컴퓨터 관련 증거, 컴퓨터 전자기록 등의 용어로 부르기도 한다. 디지털 증거에 대하여 탁희성은 각종 디지털 매체에 저장되거나 네트워크 장비 및 유·무선 통신상으로 전송되는 정보 중 그 신뢰성을 보장할 수 있어 증거로서의 가치를 지니는 디지털

정보라고 정의하였다[2]. 양근원은 범죄와 피해자 또는 범죄와 가해자 사이의 연결고리를 제공할 수 있는 모든 디지털 데이터를 말한다고 하였다. 또한 여기에서 디지털 데이터란 전통적 의미의 컴퓨터상에 있는 데이터뿐만 아니라 이진 형태로 저장되거나 전송될 수 있는 모든 텍스트, 이미지, 오디오 및 비디오 데이터를 포함한다고 정의하였다[3][4]. 권오걸은 특정한 정보를 담고 있는 저장매체 또는 특정한 정보를 전송하는 전송매체가 디지털의 형태를 가지고 있는 경우를 디지털 증거라고 할 수 있다고 정의하였다[5]. 디지털 증거는 아날로그 증거와 다르게 매체독립성, 대량성, 복제성, 취약성, 비가시성, 익명성의 특징을 가지며 특징과 설명은 다음 <표 1>과 같다.

<표 1> 디지털 증거의 특징

특징	내용
매체 독립성	저장매체나 매개체의 특성에 따른 영향을 받지 않고 항상 일정한 정보의 값을 유지함
대량성	데이터의 양이 방대하여 특별한 기술과 도구, 교육된 전문가 없이는 증거추출이 곤란함
복제성	반복된 복사과정을 거치더라도 디지털 정보의 값 혹은 가치가 동일하게 유지되므로 질적인 면에서 원본과 사본의 구별이 어려움
취약성	간단한 조작만으로 위·변조가 가능하고 정보일부의 삭제 혹은 변경이 용이함
비가시성	전자적 정보의 형태로 기록, 저장되기 때문의 인간의 오감으로는 직접 정보의 내용을 인지할 수 없음
익명성	작성자 또는 소유자를 확인하는 것이 불가능한 경우가 많음

2.3 메타분석

1976년 Glass에 의해 처음으로 소개된 메타분석은 그 이후 많은 연구자들이 연구방법으로 활용하고 있다. Field에 의하면 1981년부터 2000년 사이 2,200편 이상의 메타분석에 관한 연구가 출판될 정도로 그 활용 빈도가 매우 높은 연구 방법이라고 할 수 있다[6][7][8].

메타분석은 종합적 메타분석과 분석적 메타분석으로 구분할 수 있다. 연구의 전반적인 주제와 방법들을 분석하여 특정 연구 영역의 연구방향이 어떻게 진행되고 있는지 살펴보기에 적절한 종합적 메타분석이다. 반면 분석적 메타분석은 한 가지 개념이나 주제에 관해 집중적으로 분석하며, 동일한 주제를 다룬 연구들을 분석 단위로 삼아 측정한 결과를 통합적으로 다시 살펴보는 연구이다[9].

메타분석의 필요성을 요약하면 다음과 같다. 첫째, 하나의 주제에 관해 서로 상이한 결론이나 논쟁이 야기될 때, 이를 해결하기 위한 신뢰성과 타당성이 있는 대결론을 내려야 할 필요가 있는 경우에 효과적이다. 둘째, 원 자료를 수집할 만한 시간적 여유가 없거나, 경비와 노동력의 절약이 요구되는 상황에서 2차 자료를 이용한 문제를 해결할 경우에 필요하다. 셋째, 수많은 학술 정보 속에 체계적인 절차를 통한 압축된 지식이나 정보들을 필요로 할 경우 효과적이다[10].

3. 연구방법론

3.1 분석대상

본 연구는 2006년부터 2016년까지 총 11년에 걸쳐 발표된 국내 학술지에 게재된 총 94편의 논문을 분류하고 분석하였다. 한국정보보호 학회의 논문지인 '정보보호학회논문지'와 한국 디지털포렌식학회의 논문지인 '디지털 포렌식 연구'에 게재된 국내 학술지 논문을 대상으로 자료를 검색하였다. 정보보호학회논문지는 1991년부터 현재까지 총 125호가 발행되었으며, 정보보호(암호학, 정보통신공학, 전산학, 수학 등)에 관련된 학문적 연구논문들이 게재되고 있는 학술지이다. 디지털 포렌식 연구는 2007년부터 현재까지 총 15호가 발행되었으며, 디지털 포렌식에 관련된 법률·기술적 학문 연구논문들이 게재되고 있는 학술지이다. 물론, 디지털 포렌식과 관련된 연구가 학술지 외에 단행

본, 학위논문 등의 형태로도 수행되고 있을 것이다. 그러나 국내에서 디지털 포렌식에 대한 연구의 역사가 깊지 않고, 연구결과물의 물리적인 양도 많지 않다. 이 때문에 학술지에 게재된 논문을 중점으로 메타분석을 진행하여도 국내 디지털 포렌식 연구동향을 파악하는 데 무리가 없이 충분한 의미를 가질 것으로 판단하였다.

3.2 분류기준

본 연구의 분석대상으로 수집된 논문을 분류하기 위해 메타분석을 진행한 6개 논문의 분류기준에 대해 선행연구를 진행하였다.

김훈순은 텔레비전 서사연구에 대한 메타분석을 진행한 연구에서 연구주제, 연구목적, 연구방법으로 논문을 분류하였다[11]. 황상재는 국내 인터넷 연구에 대한 메타분석을 진행한 연구에서 연구주제, 연구방법으로 분류하였다[12]. 김성태는 국내 내용분석 연구에 대한 메타분석을 진행한 연구에서 연구방법으로 논문을 분류하였다[13]. 김광재는 혁신의 확산 연구에 대한 메타분석을 진행한 연구에서 연구주제, 연구목적, 연구방법, 연구대상을 분류기준으로 선정하였다[14]. 류준호는 문화콘텐츠 관련 연구에 대한 메타분석을 진행한 연구에서 연구목적, 연구분야, 연구방법으로 논문을 분류하였다[9]. 강미화는 보안경제성에 대한 연구동향을 분석한 연구에서 연구주제, 연구방법을 분류기준으로 선정하였다[15].

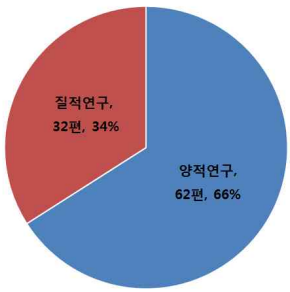
본 연구에서는 6개의 선행연구 논문 중 4개 이상의 논문에서 채택한 기준을 사용하여 논문을 분류하고자 하였다. 그리하여 도출된 분류기준은 연구방법과 연구주제로, 선행연구 논문 중 각 4개, 6개의 논문에서 선정한 분류기준이다. 본 연구의 연구방법별 분류기준은 메타분석 선행연구 논문에 따라 양적연구와 질적연구로 설정하였다. 본 연구의 연구주제별 분류기준은 디지털 포렌식 절차에 근거하였다. 디지털 포렌식 절차는 관련 법 준수를 바탕으로 증거수집, 증거보존, 증거분석, 법정제출에 이르게 된다. 이에 따라 본 연구에서는 연구주제별 분류기준을 크게 법, 관리, 기술로 설정하였다. 그리고 각 주제별 하위주제로는 법, 증거수집관리, 증거보존관리, 증거분석관리, 증거수집기술, 증거보존기술, 증거복구기술, 증거분석기술로 설정하고 분류하였다.

4. 디지털 포렌식 연구동향 분석

국내 디지털 포렌식 관련 연구동향을 분석하기 위하여 국내 학술지인 '정보보호학회논문지'와 '디지털 포렌식 연구'에서 자료를 수집하여 분석하였다. 2006년부터 2016년까지 수집된 자료 중 디지털 증거를 대상으로 한 연구는 총 94편이었다. 본 연구의 분석대상으로 선정된 논문은 크게 연구방법별, 연구주제별로 분석하였고, 추가적으로 각 연구에서 주제로 선정한 상세 키워드가 무엇인지 추출하여 분석하였다.

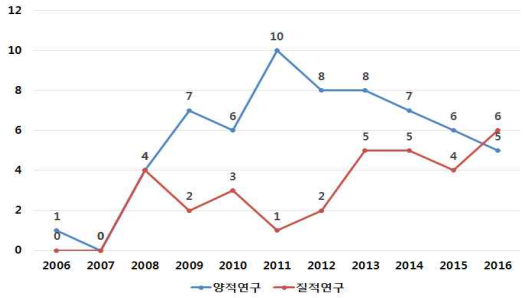
4.1 연구방법별 분류

수집 논문을 2개의 연구방법 기준으로 분류하여 빈도를 분석한 결과, 양적연구로 연구를 진행한 논문이 62편으로 66.0%를 차지하였다. 질적연구로 연구를 진행한 논문은 32편으로 34.0%로 그 뒤를 따른다.



(그림 1) 연구방법별 논문 비율

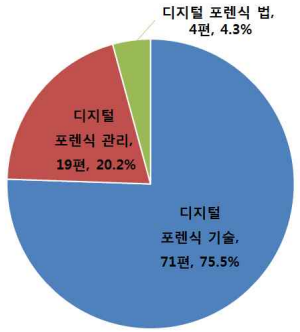
연구방법별로 연도에 따른 변화를 살펴보면, 본격적으로 연구가 시작되는 2008년에는 양적연구와 질적연구의 수가 동일하였다. 그러나 2012년까지 질적연구가 계속적으로 하락하는 형태를 보이고, 양적연구는 2011년까지 증가하는 형태를 보이며 2011년에 급상승하여 가장 많은 연구결과를 내었다. 그러나 2012년 이후 양적연구가 하락하고 질적연구가 상승하는 반대적인 양상을 보이며 2016년에는 처음으로 질적연구가 양적연구를 앞서게 되었다. 연구방법별 연도에 따른 논문 수는 아래 (그림 2)와 같다.



(그림 2) 연도별 논문 수(연구방법)

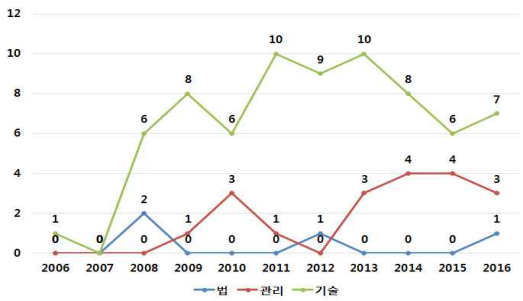
4.2 연구주제별 분류

우선적으로 법, 관리, 기술 3개의 기준으로 분류하여 빈도를 분석한 결과, 기술을 주제로 한 논문이 71편으로 75.5%를 차지하여 가장 많았다. 관리를 주제로 한 논문은 19편으로 20.2%, 법을 주제로 한 논문은 4편으로 4.3%로 그 뒤를 따른다. 앞서 디지털 포렌식 기술력의 진보에 비해 법과 제도의 확립이 부족한 실정이라고 언급한 것과 같은 맥락으로 기술 주제의 논문이 압도적인 비율을 차지하는 것을 알 수 있다. 총 94편의 논문 중 단 4편만이 디지털 포렌식 관련 법을 주제로 진행한 연구이었으므로, 법과 관리 주제에 대한 연구의 활성화가 시급하다고 사료된다.



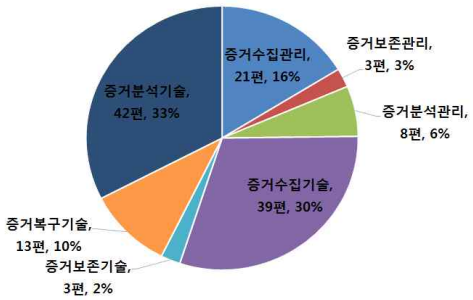
(그림 3) 연구주제별 논문 비율

연구주제별로 연도에 따른 변화를 살펴보면, 법을 주제로 한 논문은 매년 0편에서 2편이 게재되고 있다. 이를 통해 상대적으로 가장 연구가 부족한 주제가 디지털 포렌식 관련 법이라는 것을 알 수 있다. 관리를 주제로 한 논문은 2008년부터 2010년까지 0편에서 3편으로 상승하다가 2012년에 다시 0편으로 하락하였다. 그러나 2013년부터 2016년까지 3편 이상의 논문이 게재되고 있다. 기술을 주제로 한 논문은 본격적으로 연구가 시작된 2008년부터 2013년까지 지속적으로 매년 6편 이상의 논문을 게재하였으며, 2011년과 2013년에는 10편의 디지털 포렌식 기술 논문이 출판되었음을 알 수 있다. 그러나 그 이후로는 하락하는 양상을 보이며 2015년에는 관리 논문과의 편차를 가장 많이 좁혔으나, 2016년에는 다시 상승하고 있다.



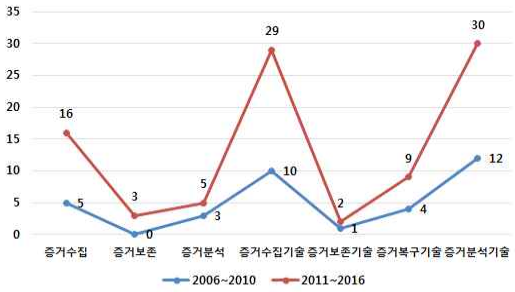
(그림 4) 연도별 논문 수(연구주제)

다음으로 3가지 상위주제로 분류 후, 8가지 하위주제로 분류하여 분석한 결과는 아래와 같다. 증거분석기술을 주제로 한 논문이 42편으로 32.6%의 비율로 가장 많았고, 증거수집기술을 주제로 한 논문이 39편으로 30.2%를 차지하며 뒤를 이었다. 다음으로는 증거수집관리를 주제로 한 논문이 21편으로 16.3%, 증거복구기술을 주제로 한 논문이 13편으로 10.1%, 증거분석 관리를 주제로 한 논문이 8편으로 6.2%, 증거보존관리와 증거보존기술을 주제로 한 논문이 각각 3편으로 2.3% 순이었다. 전체 하위주제별 논문 비율과 수는 다음 (그림 5)와 같다.



(그림 5) 전체 하위주제별 논문 비율과 수

전반적인 연구동향을 파악하기 위해, 5~6년 단위로 나누어 2006년에서 2010년까지, 2011년에서 2015까지 그룹을 지어 시간의 흐름에 따른 하위주제별 연구추이를 분석하였다. 논문 수에서는 차이가 나지만 전체적인 연구동향은 동일하다고 해석할 수 있다. 두 그룹에서 모두 증거분석기술과 증거수집기술에 대한 연구가 가장 활성화되었다고 분석되었으며, 다른 하위주제에 대한 연구가 상대적으로 부족하여 향후 유망한 주제가 될 수 있을 것이라고 사료된다. 또한 전반적인 논문 수를 살펴보았을 때, 모든 하위주제에서 2006년에서 2010년까지의 논문 수에 비해 2011년에서 2016년까지의 논문 수가 증가하였음을 알 수 있다. 이 점을 미루어 보면 디지털 포렌식에 대한 연구가 점차 활발해지고 있음을 짐작할 수 있다.

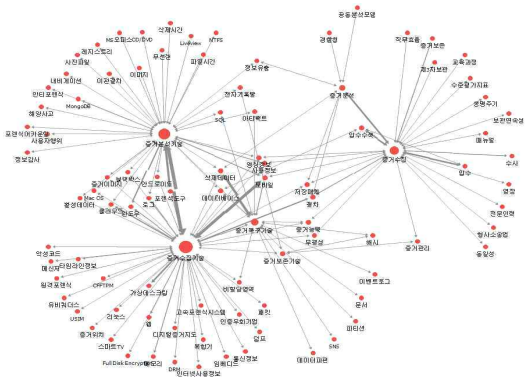


(그림 6) 연도별 논문 수(하위주제)

상위주제별로 상세하게 살펴보면 기술주제에서 연구가 가장 활성화된 하위주제는 증거분석기술이었으며, 작은 차이로 증거분석기술이 두 번째로 활성화된 주제로 분석되었다. 그 뒤로는 증거복구기술, 증거보존기술 순이었다. 증거분석기술과 증거수집기술을 주제로 한 논문의 비율이 80% 이상을 차지하기 때문에, 기술이라는 상위주제에서 대부분의 논문이 증거분석과 증거수집이라는 기술에 대해 연구를 진행한 것을 알 수 있다. 증거를 수집하고 분석하는 것이 디지털 포렌식 기술에서 가장 주요한 기술이지만 증거복구, 증거보존과 같은 다른 기술에도 많은 연구가 필요하다고 사료된다.

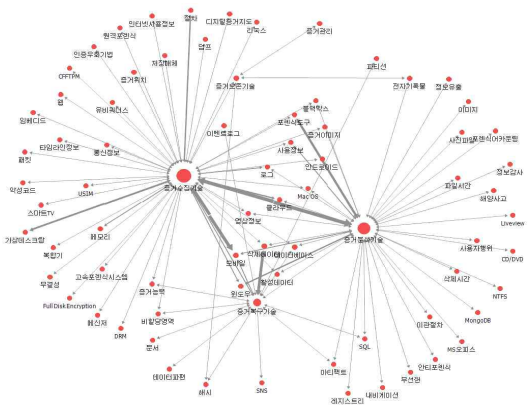
관리주제에서 가장 활성화된 하위연구주제는 증거수집으로, 과반 이상인 65.6%의 비율로 분석되었다. 그 뒤로는 증거분석관리 25.0%, 증거보존관리 9.4% 순이었다. 증거분석기술의 연구가 가장 활성화된 기술주제와는 다르게 상당수의 논문이 증거수집에 대한 연구를 진행했음을 알 수 있다.

또한 각 하위주제에서도 어떤 키워드의 연구가 진행되고 있는지, 키워드간의 연관성은 어떠한지 살펴보기 위하여 관계데이터에 대한 분석을 수행하는 도구인 넷마이너를 이용하여 연관성을 분석하였다. 전체 논문의 연관성 분석 결과는 아래 (그림 7)과 같다.



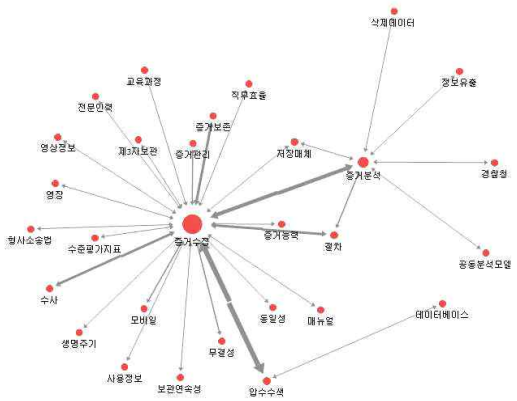
(그림 7) 전체 논문 연관성 분석

기술 주제의 논문에 대한 연관석 분석 결과는 증거수집기술과 증거분석기술간의 연관성이 매우 높은 것으로 나타났는데, 이는 한 논문에서 증거수집과 증거분석에 대한 기술을 함께 연구한 경우가 많기 때문이다. 연구가 가장 활성화되었다고 분석된 증거분석기술은 '포렌식 도구', '윈도우' 키워드와 연관성을 지니고 있는 것으로 나타났는데, 이는 증거분석에서 포렌식 도구는 필수적인 기술요소이기 때문인 것으로 사료된다. 또한 국내에서는 윈도우 운영체제의 사용이 보편화되어있기 때문에 윈도우 운영체제상에서의 증거분석기술 연구가 활성화 되어있다고 분석된다. 다음으로 증거수집기술은 '모바일', '절차', '가상데스크탑', '클라우드'키워드와 연관성이 있는 것으로 분석되었다. 모바일, 가상데크스탑, 클라우드 등과 같은 새로운 저장매체로 부터의 증거수집에 대한 기술이 주목받고 있는 것을 알 수 있는 대목이다. 그 중에서도 모바일에서 증거수집을 수행하는 기술에 대한 관심이 매우 높은 것으로 보인다. 증거복구기술은 '삭제데이터'와 깊은 연관성을 가지고 있는 것으로 분석되었다. 디지털 매체에서 삭제된 데이터를 복구하는 기술에 대해 조사하는 연구자가 많은 것을 알 수 있다.



(그림 8) 기술주제 논문 연관성 분석

관리주제의 논문에 대한 연관성 분석결과 연구한 논문의 수가 가장 많은 증거수집 주제는 '압수수색', '수사', '절차'등의 키워드와 깊은 관련성이 존재하는 것으로 나타났다. 다른 주제들과는 다르게 증거수집에 대한 연구에서는 수사와 관련된 키워드가 두드러지게 드러났다. 우선적으로 가장 두터운 연관성을 보인 압수수색은 디지털 포렌식 수사 절차 상 가장 앞서 진행되는 단계이다. 수사를 위한 증거수집은 압수수색을 통하여 진행되고, 그에 대한 절차에 대한 연구가 상당수 진행된 것을 분석결과를 통해 알 수 있다.



(그림 9) 관리주제 논문 연관성 분석

5. 결론

본 연구는 디지털 포렌식 관련 연구에서 그동안 진행된 연구의 흐름을 파악하고 향후 유망한 연구의 주제를 찾고자하였다.

‘정보보호학회논문지’와 ‘디지털 포렌식 연구’, 2개 학술지에서 2006년부터 2016년까지 총 11년 동안 발표된 논문들을 대상으로 연구의 주제와 방법론을 중심으로 디지털 포렌식 관련 연구에 대한 정량적인 분석을 시도하였다. 본 연구의 결과, 디지털 포렌식 관련 연구는 기술주제의 논문이 대부분인 것으로 나타났다. 그러므로 디지털 포렌식 관리와 관련 법에 대한 연구가 적잖이 진행되어야 할 것으로 생각된다. 또한 기술, 관리, 법의 하위 주제에 대한 분석에서는 증거분석기술, 증거수집기술, 증거수집관리, 증거복구기술 등의 주제로 진행한 연구가 많았다. 연구방법별로 분류하였을 때 연구자들이 가장 선호하는 연구방법으로 양적연구임이 드러났다. 또한 주제별로 키워드 분석을 수행하였다. 기술주제에 대한 키워드 분석결과는 다음과 같다. 증거분석기술에서 많이 등장한 키워드는 포렌식 도구, 윈도우, 증거이미지, 사용정보, 모바일로 증거를 분석하는 환경과 분석 시 사용하는 도구, 분석 대상이 주로 등장하는 것을 알 수 있다. 그 중 가장 많이 등장한 키워드는 포렌식 도구로 디지털 포렌식 분석 시 도구가 가장 중요하다는 것을 추측할 수 있다. 증거수집기술에서 많이 등장한 키워드는 가상 데스크탑, 절차, 모바일, 메모리, 클라우드로 증거를 수집해야하는 대상이 키워드로 주로 등장하는 것을 알 수 있었다. 그 중 가장 많이 등장하는 키워드는 모바일로 스마트폰의 등장과 함께 디지털 포렌식을 이용한 범죄수사에서 모바일에서 획득한 증거가 많이 사용됨을 추측할 수 있다. 또한 증거수집기술과 증거분석기술은 매우 큰 연관성을 보였는데, 이는 대상에 따라 증거를 수집하고 분석하는 연구를 함께 진행한 연구가 많았음을 알 수 있다. 증거복구기술에서 많이 등장한 키워드는 삭제데이터로 디지털 증거를 복구하는데 있어서 삭제데이터가 가장 큰 이슈라는 것을 추측할 수 있다. 또한 상대적으로 증거보존기술은 다른 기술들에 비해 연구가 활성화되지 않은 것으로 볼 수 있었는데, 모든 기술의 균형을 위해 증거보존기술에 대한 연구가 유망한 연구 주제가 될 것이라고 판단하였다. 관리주제에 대한 키워드 분석결과는 다음과 같다. 증거수집관리에서 많이 등장한 키워드는 수사, 절차, 무결성, 증거관리 등으로 증거를 수집하는 절차와 수사에서 증거의 무결성이 갖는 중요성이 증거수집관리에서의 주요 연구동향임을 알 수 있다. 또한 증거수집관리는 압수수색, 증거분석과 매우 큰 연관성을 보였는데, 이는 압수수색에서 증거수집, 증거수집에서 증거분석으로 이어지는 디지털 포렌식 절차가 매우 밀접하게 연결되어있음을 알 수 있다.

본 연구는 연구대상에 특정 학술지만을 포함하였다는 점, 주제 및 연구방법만으로 분석하였다는 점으로 인해 한계가 있으나, 정량적인 분석을 통해 디지털 포렌식 관련 연구동향을 파악하였다는 점에서 의의를 가진다.

본 연구의 결과는 디지털 포렌식 관련 연구에 관심이 있는 연구자들이 연구동향 파악, 연구방향 설정 등을 하는 데 도움이 될 것으로 기대된다. 향후 연구에서는 더욱 다양한 학술지로 연구범위를 확대 하고자 한다. 그러나 이 과정에서는 각 학술지에서 디지털 포렌식 관련 연구를 찾아내는 과정에 어려움이 수반 될 것이라고 예상된다. 향후 연구에서는 분류기준을 다양화하여 학술지, 저자정보, 연구대상, 연구목적 등에 따른 디지털 포렌식 관련 연구동향을 분석하고자 한다. 이러한 심층적인 분석을 통해서는 현재까지의 연구동향 파악하는 것에서 더 나아가 향후 디지털 포렌식 관련 연구동향을 예측해 볼 수 있을 것이다. 또한, 정량적인 분석에 대상이나 과정의 내용과 특징을 있는 그대로 열거하거나 기록하여 서술하는 기술적인 성격을 더한다면 더욱 의미 있는 연구가 될 것으로 기대된다.

참고문헌

[1] 신용태, “디지털증거의 무결성 유지를 위한 절차와 사례에 관한 연구”, 대검찰청, 2006.
[2] 탁희성, 이성진, “디지털 증거분석도구에 의한 증거수집절차 및 증거능력 확보방안”, 한국형사정책연구원 연구총서, pp.6-21, 2006.
[3] 양근원,. “디지털 증거의 특징과 증거법상의 문제 고찰”, 한국경찰학회보, 제12권, pp.133-166, 2006.
[4] 양근원, “형사절차상 디지털 증거의 수집과 증거능력에 관한 연구”, 경희대학교 박사학위논문, 2006.
[5] 권오걸, “디지털증거의 개념·특성 및 증거능력의 요건”, IT와 법 연구, 제5집, pp.291-318, 2011.
[6] Glass, G. V., “Primary, secondary, and meta analysis of research”, Educational Researcher, Vol.5, pp.3-8. 1976.
[7] Field, Andy P, “Meta-analysis of correlation coefficients: a Monte Carlo comparison of fixed and random effects methods”, Psychological Methods, Vol6, No.2, pp.161-180, 2001.
[8] 노정순, “문헌정보분야에서 메타분석 연구에 관한 고찰”, 한국문헌정보학회지, 제42권, 제1호, pp.46-61, 2008.
[9] 류준호, 윤승금, 이영주, “문화콘텐츠 관련 연구에 대한 메타분석”, 언론과학연구, 제10권, 제1호, pp.124-165, 2010.
[10] 오성삼, “메타분석의 이론과 실제”, 건국대학교 출판부, 2008.
[11] 김훈순, “텔레비전 서사연구의 메타분석”, 방송통신연구, 통권 제59호, pp.167-197, 2004.
[12] 황상재, 박석철, “국내 인터넷 연구의 메타분석 - 연구 주제와 방법을 중심으로”, 한국방송학보, 제18권, 제2호, pp.68-92, 2004.
[13] 김성태, “국내 내용분석 연구의 방법론에 대한 고찰 및 제언”, 커뮤니케이션 이론, 제1권, 제2호, pp.39-67, 2005.
[14] 김광재, “혁신의 확산 연구에 대한 메타분석”, 한국언론학보, 제54권, 제2호, pp.31-56, 2010.
[15] 박광민, 홍승완, 김종필, 장항배. “정보유출방지를 위한 디지털 포렌식 기술 비교분석 연구”, 융합보안논문지, 제16권, 제7호, pp.93-100. 2016.
[16] 강미화, 김태성, “보안경제성 연구동향 분석”, 정보보호학회논문지, 제25권, 제6호, pp.1561-1570. 2015.
[17] 이동휘, 윤주희, 김미선, “활성 포렌식 기술을 활용한 피해 유형별침해사고 대응 절차 연구”, 융합보안논문지, 제16권, 제4호, pp. 69-78. 2016.

[저자소개]

류 보 라 (Bora Ryu)

2014년 08월 상명대학교 경영학 학사
2017년 02월 중앙대학교
산업보안융합보안학 석사
2017년 03월 (주)더존비즈온
포렌식센터 연구원
email : bora0102@douzone.com

전 민 서 (Minseo Jeon)

2015년 08월 명지대학교
문헌정보학 학사
2016년 03월 중앙대학교
산업융합보안학
석사과정
email : jms2381@cau.ac.kr

지 주 연 (Juyeon Ji)

2017년 02월 성결대학교
멀티미디어공학 학사
2017년 03월 중앙대학교
산업융합보안학
석사과정
email : juyeonie@cau.ac.kr

이 찬 우 (Chanwoo Lee)

1985년 02월 한국항공대학교
전자공학 학사
2002년 02월 헬싱키 경제경영대학원
MBA
2015년 03월 중앙대학교
융합보안학 박사과정
email : chanlee114@cau.ac.kr

장 항 배 (Hangbae Chang)

2006년 02월 연세대학교
정보시스템관리 박사
2007년 03월 대진대학교
경영학과 조교수
2012년 03월 상명대학교
경영학과 조교수
2014년 03월 중앙대학교
산업보안학과 부교수
email : hbchang@cau.ac.kr