연구논문 정보화정책 제24권 제3호, 2017년 가을호, pp. 91–107

메타스터디를 통한 국내 디지털 포렌식 연구 동향

곽 나 연*, 이 중 정**, 맹 윤 호***, 조 방 호****, 이 상 은*****

요 약 디지털 포렌식이란, 디지털자료를 수집, 분석, 보고하여 법적 효력을 갖도록 하는 기술로써, 정보통신기술의 발달에 따라 국내·외 시장이 꾸준히 성장하고 있다. 이와 같은 디지털 포렌식 시장 트렌드를 반영하여 미국을 비롯한 많은 국가들이 디지털 증거의 수집과 분석에 활발한 연구를 진행 중이고, 국내 역시 디지털 포렌식 관련 학술연구가 활발하게 진행되고 있다. 따라서 관련 연구 동향과 성과를 체계적으로 분석하여 디지털 포렌식 연구의 전반적 연구경향과 성과를 확인하고, 향후 연구방향의 제언을 위한 메타분석이 필요한 시점이다. 본 논문은 지난 10년간(2007~2016) 발간된 KCI 저널 논문 470개 중, 포렌식 연구 정의에 맞는 239개를 선정하여 이를 대상으로 '대주제, 분석단계, 기술분야, 저자소속, 분석단위, 연구방법' 등의 측면에서 디지털 포렌식 연구 분야를 분석하였으며 이를 통해 국내 디지털 포렌식 연구의 중요한 연구 경향을 정리하였다. 본 분석을 통해 국내 디지털 포렌식 연구가 관련 기술 위주의 학계 주도적 특성을 보이는 것을 확인하였으며, 이를 통해 추후 연구의 발전 및 활성화를 위한 방향을 제안하였다.

주제어: 디지털 포렌식, 디지털 증거, 포렌식 기술, 포렌식 연구, 메타스터디

A Meta Study on Research Trend of Digital Forensic in Korea

Kwak, Na-Yeon, Choong C. Lee, Maeng, Yun-Ho, Cho, Bang-Ho, Lee, Sang-Eun

Abstract Digital forensics is the process of uncovering and interpreting electronic data and materials found in digital device in relation to crime. The goal of the process is to preserve any evidence in its most original form which shall be having the force of law. The digital forensic market is increasing with a growth of ICT in domestic and global market. Many countries including U.S. are actively performing researched regarding a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events which so does in academic society in Korea. This paper is to understand overall research trend about digital forensics and derive future strategy by integrating the result of meta-analysis into practices based on five criteria – main theme and topic, analysis phase, technical method for analysis, author's affiliation, and unit of analysis and method. 239 papers are analyzed, which were selected out of 470 papers published for 10 years (2007~2016) in academic journal on the list of KCI (Korea Citation index). The results of this analysis will be used to examine the characteristics of research in the field of digital forensics. The result of this research will contribute to understanding of the research trend and characteristics leading the technology-driven academia, through which measures for further research development and facilitation are suggested.

Keywords: digital forensics, digital evidence, forensic technology, forensic study, meta study

2017년 8월 24일 접수, 2017년 8월 28일 심사, 2017년 9월 14일 게재확정

* 연세대학교 정보대학원 박사과정(nnayun@gmail.com)
** 교신저자, 연세대학교 정보대학원 교수(cclee@yonsei.ac.kr)
*** IBM Watson(yunho0130@gmail.com)
**** 연세대학교 정보대학원 박사과정(harold1@naver.com)
***** 연세대학교 정보대학원 석사과정(go20002002@naver.com)

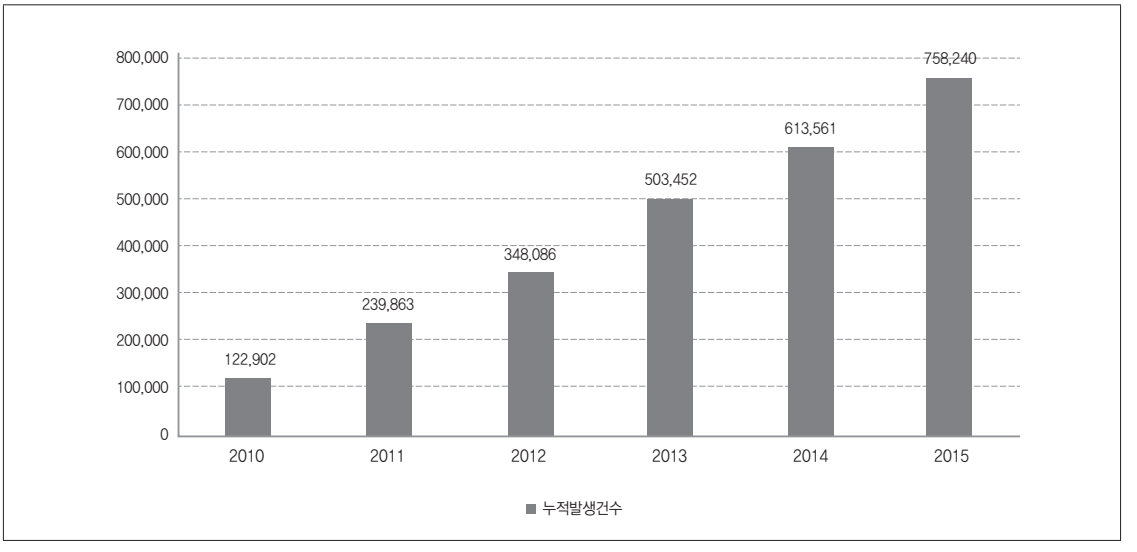
Ⅰ. 서론

1. 연구 배경 및 목적

ICT 및 인터넷 기술 발전으로 사이버 공간이 창출되고 이로 인해 수많은 개인과 기업에게 새로운 서비스 혜택과 사업기회를 제공하였다. 하지만 사이버 공간은 긍정적인 측면만 있는 것은 아니다. 사이버 범죄로 인해 개인 및 기업에게 심각한 피해 발생시키고 있다. Symantec(2016)의 보고서에 따르면, 2015년 기준 4억 3,000만개의 신규 악성코드가 발견되었으며, 이 중 제로데이 취약점은 125%이상 증가하였다. 특히 국내의 경우도 사이버 범죄가 지속적으로 증가하고 있으며, 2015년 기준 누적 사이버 범죄 발생건수는 약 76만 건에 이르고 있다(경찰청 사이버안전국, 2016). 하지만 사이버 범죄 증가에 비해 검거율 감소하고 있는데, 과거 2007년 89%에 이르던 검거율을 최근 2015년에는 73%까지 감소하였다(이대명, 2016).

이와 같은 사이버 범죄율의 증가와 낮은 검거율로 사이버 범죄의 심각성이 대두됨과 동시에 사이버 범죄 검거에 있어 디지털 포렌식 방법론이 주목 받기 시작하였다. 특히 사이버 범죄의 경우는 일반 형사 사건에 비해 증거확보가 어려운 이유로 사이버 범죄 수사의 경우 대부분 디지털 포렌식 방법이 적용된다.

디지털 포렌식이란, 디지털자료를 수집, 분석, 보고하여 법적 효력을 갖도록 하는 기술이다. 그 동안 사이버 범죄의 증거물을 디지털 포렌식 기법을 활용하여 복구하여 확보하더라도, 이에 대한 법률적 증거 효력 확보에 어려움이 있었다. 하지만, 지난 2016년 5월, 국회 법제사법위원회 제1소위원회에서 디지털 증거가 법률적 증거능력을 확보할 수 있도록 형사소송법이 개정되면서, 사이버범죄 수사에 디지털 포렌식이 적극적으로 활용될 수 있는 법률적 근거가 마련되었다. 이로써 디지털 포렌식 활용 뿐만 아니라 그 시장이 성장할 수 있는 기반이 마련되었으며, KISTI의 연구[1]에서 국내 디지털 포렌식 시장은 2019년까지 연평균 22.9%로 성장



〈그림 1〉 누적 사이버범죄 발생 건수

1) 한국과학기술정보연구원 (2014). 「Market Report : 법과학(Forensic science) 감식 제품 및 서비스 – 국내 민간 시장 활성화 통한 성장기대」. 서울: 한국과학기술정보연구원

하고, 500억원이상 규모로 성장할 것으로 예측하였으며, Globe Newswire의 시장 보고서[2]에 따르면, 글로벌 디지털 포렌식 시장이 연평균 11.4%씩 성장하여 2021년에는 약 50억 달러에 이를 것으로 추산하고 있다.

이와 같이 디지털 포렌식 시장의 성장성이 예측되고, 실제로도 성장함에 따라, 관련된 연구도 다수 진행되었다. 하지만 현재까지 연구의 대부분은 디지털 포렌식의 기술적 연구(윤종철 외, 2016; 이경식, 2016; 연규철 외, 2016)와 디지털 포렌식의 절차에 관한 연구(윤신자 외, 2013; 장성민 외, 2015)가 대부분을 차지하고 있다. 하지만 기존 연구는 기술적 측면으로 편향되어 있으며, 전반적인 포렌식 연구동향과 그 방향을 제시하는 연구는 미흡한 실정이다.

따라서 본 연구는 현재 편향되고 있는 디지털 포렌식 연구의 문제를 인식하고, 디지털 포렌식 연구의 확장성과 다양성 확보에 기여 하고자 하며, 특히 본 연구는 최근 10년간 디지털 포렌식 연구동향 분석결과를 기반으로 향후 디지털 포렌식 연구 방향을 제시하는데 주된 목적이 있다

Ⅱ. 디지털 포렌식 연구동향

1. 디지털 포렌식의 정의

포렌식은 증거를 수집하고 보존하여 처리하는 과정에서 법정에서 증거로 활용할 수 있도록 과학적·기술적인 기법을 사용하되 증거의 가치가 상실되지 않도록 하는 일련의 절차를 의미한다. 기존 포렌식은 법의학 분야 내 DNA 감식, 변사체 감시 등에 사용되었으나 컴퓨터 범죄의 증가와 함께 컴퓨터 포렌식이 생겨났으며, 초창기 컴퓨터 포렌식은 컴퓨터 중심 증거 확보에 주목하였으나, 점차 증거를 포함하고 있는 분석대상이 컴퓨터에서 다양한 디지털 장비로 확대되며 컴퓨터 포렌식에서 디지털 포렌식으로 변화하게 되었다(탁희성, 2008). 또한 디지털 포렌식은 다양해지는 사이버 범죄에 대처하기 위해 과학수사와 수사과학 분야에서 필요한 새로운 형태의 범죄 과학 분야로써 디지털 증거 수집단계에서부터 재판에 증거가 제출되어 채택되기까지, 전 과정에서 기술적, 법률적 체계로 다뤄지고 있다(양근원, 2006). 따라서 디지털 포렌식은 범죄 현장에서 확보된 디지털 증거의 보존, 수집, 증명, 식별, 분석, 해석 후 이를 기록하고 증거로 제출하기 위한 과학적 절차와 방법이라 정의할 수 있다.

2. 디지털 포렌식 국내 연구 동향

국내 디지털 포렌식 연구 분야에서 진행되고 있는 연구는 먼저 디지털 포렌식 기본 원칙과 절차, 둘째 디지털 포렌식 유형, 마지막으로 기술도구 효과성 측면으로 구분할 수 있다.

1) 디지털 포렌식 원칙과 절차

디지털 포렌식 연구에서 원칙은 수사준비, 증거물 획득, 증거물 분석, 증거물 보관, 보고의 다섯 단계로 구분하고 있으며, 각 단계에서는 지켜져야 할 원칙은 다음과 같이, 정당성, 재현성, 신속성, 연계보관성, 무결성의 5가지로 규정하고 있다. 특히 기존 연구에서 주장하고자 하는 디지털 포렌식의 원칙과 절차는 디지털 증거물 수집 당시 합법적이고 절차적인 정당성 확보, 피해 당시와 동일한 결과가 도출되어야 한다는 재현성, 그리고 소멸되기 쉬운 휘발성 데이터를 신속히 수집하고 각 단계별 담당자 및 책임자의 명확성, 마지막으로 수집된 증거가 위·변조가 없는 무결성이 증명되어야 한다(신용태, 2006). 이와 같은 연구의 주된 목적은 디지털 포렌식 기법과 이를 통해 확보된 디지털 증거의 법적인 증거능력 확보에 주된 목적이 있었다. 그리고 결과적 형사소송법 개정에 필요한 법적은 근거 마련에 기여 하였다.

2) Digital Forensics Need to cooperate with government agencies, Newswire(2015),

2) 디지털 포렌식 유형

디지털 포렌식 연구 분야는 디지털 자료의 출처 혹은 수집 및 저장매체의 특성에 따라 나누어 살펴볼 수 있다(양근원, 2006). 기존의 컴퓨터 포렌식에서 점차 확대되어 디스크 포렌식, 데이터베이스 포렌식, 시스템 포렌식, 인터넷 포렌식, 모바일 포렌식 등으로 다양한 정보보호의 응용 분야로 유형이 넓혀지고 있으며, 각 유형별 정의는 다음의 〈표 1〉과 같다.

〈표 1〉 디지털 포렌식 대상에 따른 유형별 정의

구분	정의	출처
디스크 포렌식	• 하드디스크, 플로피디스크, DVD, CD ROM 등의 물리적 저장장치와 각종 보조 기억장치에서 증거를 수집, 분석하는 포렌식 분야. • 1980년대 말부터 디스크 내 데이터를 보존, 분석하기 위한 기법이 개발되기 시작하여 현재 포렌식 분야중 가장 발전됨. • 디스크를 검색해 삭제된 파일을 복구하고, 여러 종류의 파일을 파일명, 작성자, 작성일시, 확장자 등의 기준에 따라 분류하고, 키워드 검색을 통해 수사의 단서를 추출하는 작업을 수행.	전상덕 외, 2006
시스템 포렌식	• 컴퓨터의 운영체제, 응용 프로그램 및 프로세스를 분석하여 증거를 확보하는 포렌식 분야. • 분석 대상 컴퓨터 시스템: 윈도우즈, 리눅스, 유닉스, 맥킨토시, ZENIX 등 • 사용 프로그램은 FAT16, FAT32, NTFS의 파일시스템 (Windows 운영체계), EXT(Extended File System)2 파일 시스템, EXT3 파일 시스템 (Linux) 등이 있음	전상덕 외, 2006
데이터베이스 포렌식	• 데이터베이스에서 데이터를 추출·분석하여 증거를 획득하는 포렌식 분야 • 기업의 데이터는 개인 PC와 정보 시스템 부서의 대형 시스템의 데이터베이스 내에 저장되며, 데이터 수집 및 분석에 대한 기술을 통해 기업의 분식회계, 횡령, 탈세 등 각종 범죄의 수사에 대상 기업의 정보 시스템에 저장되어 있는 데이터베이스의 분석을 수행할 수 있음	전상덕 외, 2006 이상복, 2008
네트 워크 포렌식	• 네트워크를 통하여 전송되는 데이터나 암호 등을 특정 도구를 이용하여 가로채거나 서버에 로그 형태로 저장된 것에 접근하여 분석하거나 에러 로그, 네트워크 형태 등을 조사하여 단서를 찾아내는 포렌식 분야 • IP 헤더는 목적지 IP, 발신지 IP 정보를 포함하고 있으며, 데이터 링크 헤더는 하드웨어 주소(MAC address)를 포함함. • 라우터(Router)에는 라우팅 테이블, ARP 캐쉬 테이블, 로그인 사용자, TCP 연결 관련 정보, NAT(Network Address Transla tion) 관련 정보가 포함되어 침해 시스템조사에 반드시 분석을 수행함.	전상덕 외, 2006 한국정보보호진흥원, 2003
인터넷 포렌식	• 인터넷으로 서비스되는 월드와이드웹(WWW), FTP, USENET 등 인터넷 응용 프로토콜에서 증거를 수집하는 포렌식 분야 • 웹 히스토리 분석, 전자우편 헤더 분석, IP 추적 등의 기술을 이용하여 증거 수집을 수행. • 게시판에 불법 정보 업로드나 명예훼손이 될 만한 글을 올린 용의자를 추적하기 위한 전자메일 발신자 추적, 인터넷 서핑 내역 추적 등을 진행하기 위해 웹 서버나 메일 서버, WAS(Web Application Ser ver) 등의 서버를 분석하는 작업을 통해 통하여 유용한 증거 수집 가능.	전상덕 외, 2006
모바일 포렌식	• 스마트폰, PDA, 전자수첩, 디지털 카메라, MP3 Player, 캠코더, 휴대용 메모리카드, USB 저장장치 등 휴대용 기기에 저장된 정보를 입수하여 분석하는 포렌식 분야 • 다양한 종류의 모바일 멀티미디어 기기가 개발되어 보급되고 있는 시점에서 소형의 휴대용 기기의 데이터에 대한 범죄 증거 확보의 중요성이 매우 커지고 있음.	전상덕 외, 2006

이처럼 기술의 발달과 새로운 디바이스의 출현으로 인해 정보보호의 대상과 그 유형은 계속 확장되고 있으며, 이러한 대상별 증거 수집 및 분석, 대응 방안에 대한 연구 역시 그 필요성이 증대되고 있다.

3) 디지털 포렌식 기술 도구

디지털 포렌식 절차에서 무결성을 유지하기 위해서는 크게 백업, 복구, 분석 기술이 활용된다.

휘발성을 갖는 데이터의 특성과, 데이터의 손상이나 변경을 막기 위해 백업을 위한 도구가 사용되며, 삭제되거나 손상된 데이터의 복구를 위한 도구가 사용된다. 마지막으로 수집된 데이터의 분석을 위한 도구가 사용된다(신용태, 2006). 구체적 도구의 유형은 다음 〈표 2〉와 같다.

〈표 2〉 디지털 포렌식 기술 도구 유형

유형	정의 및 활용	비고
디스크 이미징과 디스크 복제 도구	• 원본 디스크에서 증거를 추출하기 위해 바로 분석할 경우 디스크 상의 데이터의 손상이나 변경의 위험에 노출되기 때문에 원본을 물리적으로 동일한 형태로 복제하거나 (Mirror) 이미지 파일을 생성하는 도구가 필요함. • 디스크 이미징은 섹터 대 섹터 복사 또는 비트 스트림 복사 방식으로 분류 • 대부분의 이미징 도구는 원본과 동일하게 복제된 것을 입증하기 위해 CRC 체크섬(Checksum), MD5와 같은 메커니즘을 사용.	전상덕 외, 2006
데이터 무결성 도구	• 증거물이 훼손되지 않았음을 검증하기 위해 사용하는 도구. • 증거 확보나 분석 과정에서의 증거가 변경되지 않았음을 입증하기 위해 메시지 다이제스트(Message digest)나 해쉬 함수(Hash function)기법이 사용.	Stephenson, P, 2003
데이터 복구 및 분석 도구	• 디스크에서 삭제되거나 손상된 데이터를 분석하고 복구하기 위해 사용. • 파일의 MAC Time을 분석하거나 하드디스크의 파티션 테이블이 손상된 경우 사용되며, 현재 포렌식 도구 중 가장 많이 사용.	전상덕 외, 2006
암호 복구 도구	• 다양한 서버용 시스템이나 문서 파일에 암호가 설정된 경우 암호를 알아내기 위해 사용함. • 증거로 확보한 데이터나 시스템에 암호가 설정된 경우, 문서 파일 뿐만 아니라 윈도우즈 서버, 리눅스, 유닉스 등 서버용 시스템에 접근하기 위해서도 관리자나 사용자 계정이 필요함.	전상덕 외, 2006
데이터 조사 도구	• 복구된 데이터를 빠르게 확인할 수 있도록, 범용응용프로그램을 활용하거나, 키워드 검색으로 관련 문서의 추출을 용이하게 하는 것.	전상덕 외, 2006
증거 수집 도구	• 컴퓨터나 인터넷에서 증거를 수집할 때 사용. • 증거 수집을 위해 특수 목적으로 개발된 소프트웨어도 있지만 일반 범용 프로그램을 사용하기도 한다. 웹사이트 저장, 화면 캡쳐, 파일의 MAC Time 추출 등 증거 수집을 위한 많은 도구들이 존재함	전상덕 외, 2006
네트워크 및 인터넷 분석 도구	• 네트워크 트래픽을 모니터링하거나 인터넷 기반 서비스를 이용하여 증거를 수집하기 위해 사용. • 네트워크 스캐닝이나 스니핑 프로그램, 메일 추적 프로그램, 웹 히스토리 분석 도구 등을 이용	전상덕 외, 2006
데이터베이스 분석 도구	• 데이터베이스에 저장된 대용량 데이터를 분석하여 필요한 정보를 추출하기 위해 사용 • 오라클, SQL 등 데이터베이스 관리 시스템 별로 다양한 종류의 분석 도구를 사용.	전상덕 외, 2006

이처럼 유형별 포렌식 기술 도구의 정의 및 활용에 대한 연구는 현재 포렌식 연구에서 가장 활발히 진행되고 있는 분야이다. 포렌식 분석 단계가 세분화되고, 새로운 분석 대상 디바이스가 계속 등장함에 따라 이에 활용되는 분석 도구에 대한 연구 역시 꾸준히 진행되고 있으며, 기존 분석 도구나 단계의 한계를 극복하고 개선된 결과를 얻기 위해 기술 분야 연구의 중요성은 매우 높다.

3. 해외 디지털 포렌식 연구 현황

해외 디지털 포렌식 연구 현황 분석을 위해, 먼저 최근 10년(2007년~2016년) 동안 'Digital Forensics', 'Digital Evidence', 'Forensic Technology', 'Forensic Study' 등의 키워드로 출판된 자료를 검색하였다. 이 중 Conference Proceeding이거나 학위논문을 제외하고 SCI, SSCI 저널 게재 논문을 확인하였으며, 최종 1,219편의 논문을 최종 확정하였다. 출판연도별로는 2007년 43편, 2008년 55편, 2009년 87편, 2010년 88편, 2011년 94편, 2012년 121편, 2013년 151편, 2014년 154편, 2015년 189편, 2016년 237편으로 매해 출판 논문이 꾸준히 증가하고 있음을 확인하였다. 주요 출판 학술지는 Digital Investigation(269편), Forensic Science International(106편), IEEE Transactions on Information Forensics and Security(88편), Journal of Forensic Sciences(84편) 등의 학술지의 비율이 높은 것으로 확인되었다. 이와 같이 선정된 디지털 포렌식 관련 연구들의 주제들은 Computer Science(662편), Engineering(250편), Telecommunications(66편) 등에서 나타난바, 먼저 디지털포렌식 도구, 기법 및 장비/시스템 개발 그리고 모바일, SNS 등 소셜미디어 등에서 생성된 대용량 데이터의 증거, 수집, 분석을 위한 알고리즘 설계에 관한 연구가 다수 수행 되었으며, 그 다음으로 Government Law(20편), Criminology Penology (12편) 등에서 정부정책, 수사기관과 준 수사기관에서 도입사례, 형사소송법상의 증거채택 문제가 주로 다뤄졌다. 마지막으로 Business Economics(7편) 등에서 지적재산권 보호, 산업기밀 유출방지 매커니즘 및 디지털포렌식 기술진화와 사회인식 변화에 따라 새로운 비즈니스 기회 그리고 사용자 관점에서 다양한 디바이스에 적용 가능성에 대한 연구가 미약하나마 진행되고 있다.

지금까지 해외 디지털 포렌식 관련 연구는 현재 물리적 관점에서 IT 시스템과 장비 그리고 논리적 관점에서 프로세스 개선을 위한 연구에 치중되어 있다. 이와 같은 해외 연구 동향에서 살펴볼 수 있는 것처럼, 기술적 관점으로 편향되어 있다는 점에서 크게 다르지 않지만, 국내 연구동향과는 달리 디지털 포렌식의 경제, 경영학적인 시사점을 제시하는 연구가 진행되고 있다는 점이다. 이는 향후 국내 연구에서 반드시 검토되어야 할 것이다.

Ⅲ. 연구방법론

1. 메타분석 연구 방법론

메타스터디란 '연구에 대한 연구이자 분석에 대한 분석'으로 정의 할 수 있다. 이는 기존의 연구를 체계적으로 분석하여 그 경향과 특성 등을 파악하는 것이다. 이는 크게 종합적 차원과 분석적 차원으로 구분할 수 있다(Wallace, 1992; 황상재 · 박석철, 2004). 종합적 메타분석은 특정 분야의 연구방향이 어떻게 진행되었는지를 살펴보기 위해 해당 분야의 연구의 전반적인 주제나 방법 등에 대한 기준에 따라 살펴보는 것이다. 반면 분석적 메타분석은 한 가지 개념이나 주제 또는 변수를 정하고 이를 분석의 기본 단위로 집중적으로 탐구하는 것을 의미한다.

따라서 본 연구에서는 국내 디지털 포렌식 연구의 그간 연구동향을 면밀히 살펴보고 향후 연구를 위한 시사점을 찾기 위해 종합적 메타분석을 수행하였다.

특히 메타 분석의 핵심은 분석관점과 관점별 세부 분석 기준을 마련하는 것이다. 본 연구에서는 기존 메타분석의 틀로써 정보시스템 분야에서 다양하게 사용되어온 Vessey, et al.(2002)을 토대로 디지털 포렌식의 성향을 반영 할 분석 기준점들을 추가하였다. 본 연구

의 분석관점은 '연구수행 관점'과 '현장적용 관점'으로 구분하여 설정하였다. 먼저 연구수행 관점은 일반적으로 사회과학적 연구방법론에서 핵심적인 개념으로 다루고 있는 '연구주제', '방법론', '분석단위'를 포함하고, 특히 연구 주제 및 연구의 전반적 절차에 영향을 미칠 것으로 예측되는 '연구자의 소속' 또한 분석 기준으로 설정하였다. 디지털 포렌식 기법의 현장적용 관점에서 '디지털 포렌식 절차', '디지털 포렌식 대상매체 및 기술' 그리고 '법률적용 분야'를 분석 기준으로 설정하고, 최종 7가지 관점에 따라 분석을 추진하였다.

1) 분석대상 선정

디지털 포렌식은 디지털 자료를 수집 및 분석 법적 효력을 갖도록 하는 과정에서 수집 및 분석 관련 기술, 법률, 관련 사회적 이슈 등의 여러 학문분야와 관련되어 있다. 따라서 본 연구에서는 디지털 포렌식이 디지털 증거자료를 밝혀내는 공학(기술)적 분야뿐만 아니라 디지털 포렌식과 관련해 진행되는 전반적인 연구 동향을 분석하고자 한다. 분석대상 논문은 학술논문검색 및 원문 서비스를 제공하고 있는 DBPIA(www.dbpia.co.kr), NDSR(www.ndsr.kr)와 RISS(http://www.riss.kr) 서비스를 활용해 검색하였다. 먼저 최근 10년(2007년~2016년) 동안 게재된 논문을 대상으로 제목과 키워드를 검색하였다. 검색은 '디지털 포렌식', '디지털 증거', 포렌식 도구', '포렌식 절차', '증거 수집 · 분석', ' 컴퓨터 범죄', '디지털 자료' 등의 키워드로 진행하였다. 다음 단계로는 검색된 논문이 한국연구재단(KCI) 등재지 게재논문인지를 확인하였다. 마지막으로 각 저널별 최근 10년 간 논문 중, 디지털 포렌식과 관련된 연구이지만 키워드 검색에서 누락된 논문들이 있는지 확인하고 발견되는 경우 해당 논문을 분석대상에 포함시켰다. 그 결과 총 239편의 논문을 최종 확정하였다.

2) 자료분석 절차

본 연구의 분석을 위해 연구팀에서는 분석대상 논문들의 원본을 입수하여 원문 전체를 읽고 저자, 연도, 학술지, 저자 소속 등 기본항목에 대해 분류한 후, 연구주제, 연구방법, 분석단계 등 세부항목에 대해 분류하고 속성 값을 항목별로 분류하였다. 세부항목의 속성값을 부여할 때는 4명의 연구원이 2팀으로 나누어 랜덤하게 논문을 나누어 읽고 1차 분류한 후, 팀 내에서 부여된 값에 이견이 있는 경우, 해당 논문에 대한 팀 내 토론을 통해 합의하였다. 최종적으로 모든 분류항목의 속성 값을 엑셀데이터로 입력하여 빈도분석 및 교차분석을 실시하였다.

3) 메타분석 관점의 설정

(1) 연구주제

연구 주제는 각 논문이 다루고 있는 디지털 포렌식의 핵심 주제나 이슈에 대한 것을 의미한다. 본 연구에서는 Lillis, et al.(2016)의 연구에서 언급된 디지털 포렌

〈표 3〉 연구주제에 따른 분류기준

구분	세부 항목 설명
디지털 포렌식 절차	디지털 증거 처리 및 분석 과정의 표준화된 절차를 분석하고, 디지털 증거의 무결성 확보를 위한 수사 현장의 연계 관리 방법 및 디지털 증거 수사의 효율적 방안 및 절차 모델을 연구하는 연구
도메인	디지털 포렌식 도메인 전반에 대한 연구
기술	포렌식 증거 복구 수집, 분석 및 안티 포렌식 관련 기술 및 도구에 대한 연구
법률 연구	국내외 디지털 포렌식 법제 현황 과 법정에서 디지털 증거가 범죄의 증거로써 사용되기 위해 필요한 요건에 대한 연구

출처 : Lillis, et al.(2016)

식의 진행 절차, 관련 기술, 법률 연구에 대한 구분을 활용하고, 여기에 디지털 포렌식 분야 전반에 대한 내용을 추가적으로 살펴보았다. 항목별 세부적 내용은 〈표 3〉과 같다.

(2) 연구방법

연구방법의 분류는 Vessey, et al.(2002)이 제시한 분류체계인 개념적 분석(Conceptual Analysis), 수리적 분석(Mathematical Analysis), 사례연구(Case Study), 데이터 분석(Data Analysis), 현장연구(Field Study), 시스템 평가(System Evaluation), 도구개발(Instrument Development), 실험실 실험(Laboratory Experiment-human Subjects)의 내용을 검토한 후 디지털 포렌식 관련 연구에서 관련이 낮은 항목을 제외하여 〈표 4〉와 같은 기준으로 진행했다.

(3) 연구 분석단위

분석단위 역시 Vessey, et al.(2002)의 연구에서 제시한 10가지 분류 기준인 사회(Society), 전문가(Profession), 프로젝트 (Project), 조직간 환경(Inter-organizational Context), 조직 환경(Organizational Context), 그룹/팀(Group/Team), 개인(Individual), 추상적 개념(Abstract Concept), 컴퓨팅 요소(Computing Element), 컴퓨팅 시스템(Computing System) 중, 디지털 포렌식 분야 관련 연구에서 관련성과 빈도가 낮은 항목을 제외하였으며, 항목 및 세부 설명은 〈표 5〉와 같다.

(4) 연구자의 소속

연구자의 소속은 연구 주제 및 연구의 전반적 절차에 영향을 미칠 것으로 예측된다. 예를 들어, 연구자가 학계에 소속된 경우엔 연구의 주제와 그것을 확인하기 위한 방법론이 이론에 근거하여 도출되며, 공공인 경우 국가의 정책 수립과 연관한 연구 주제를 수립할 것이다. 또한 민간기업의 경우 연구의 주제가 실무적 이슈며 실용적이고 현장 활용성이 높은 기술에 대한 연구를 수행할 확률이 높다. 디지털 포렌식 분야는 범죄의 수사를 위해 수사 과정 등에서 활용되는 실용적 학문이지만, 4차 산업시대와 관련한 정부의 디지털 관련 분야 정책과 연관이 있는 학문분야이기에, 연구의 주체가 어디인지를 확인하기 위해 저자의 소속을 〈표 6〉과 같이

〈표 4〉 연구방법에 따른 분류기준

구분	세부 항목 설명
개념적분석	개념적 분류기준을 마련하여 내용분석 또는 데이터를 수집하는 연구
도구개발	저자가 직접 프로그래밍을 실시하여 툴을 개발하고 수행한 연구
시스템평가	기존에 있는 툴을 활용하여 실행가능성 및 개념구현을 확인하는 시뮬레이션 연구
설문	설문을 통한 연구
메타스터디	연구 전반에 대한 동향을 분석한 연구

출처 : Vessey, et al.(2002)

〈표 5〉 분석단위에 따른 분류기준

구분	세부 항목 설명
개인	개인을 분석 단위로 하는 연구
기관	조직 및 기관의 활용에 초점을 맞춘 연구
국가	지역적, 국가적 수준에서의 포렌식의 이슈를 고찰하는 연구
기술	특정 시스템 및 기술, 컴퓨팅 요소에 초점을 맞춘 연구

출처 : Vessey, et al.(2002)

추가적으로 확인하였다.

(5) 디지털 포렌식 절차

Vessey, et al.(2002)의 연구에서 제시된 분류기준에 추가하여 디지털 포렌식에 대한 연구 동향을 파악하기 위해 세부 항목을 구성하였다. 그 중 첫 번째는 디지털 포렌식의 수행 절차에 대한 분류로써 이형우 외(2002)의 연구에서 제시한 디지털 증거의 복구, 수집, 분석의 절차에 해당하는 논문을 구분하였으나 특정 단계가 아닌 포렌식 기술이나 분야의 전반적인 절차를 다루고 있는 연구가 많아 이를 추가하여 〈표 7〉과 같이 분류하였다.

(6) 디지털 포렌식 대상매체 및 기술

디지털 포렌식 대상 매체 및 기술은 이형우 외(2002)의 연구에서 제시한 디지털 포렌식 유형에 따라 디스크 포렌식(Disk Forensic), 네트워크 포렌식(Network Forensic), 모바일 포렌식(Mobile Forensic), 시스템

〈표 6〉 저자 소속에 따른 분류기준

구분	세부 항목 설명
공공	저자의 소속이 관공서 및 공기업, 준정부기관에 해당되는 경우
민간	저자의 소속이 민간인이 출자하여 경영하는 기업에 해당되는 경우
학계	저자의 소속이 대학 등의 학술기관에 해당되는 경우

〈표 7〉 디지털 포렌식 절차

구분	세부 항목 설명
증거 복구	디지털 증거 복구 단계 관련 연구
증거 수집	디지털 증거 수집 단계 관련 연구
증거 분석	디지털 증거 분석 단계 관련 연구
포렌식 전반	증거복구-수집-분석단계를 전반적으로 다루고 있는 연구

출처 : 이형우, 이상진, 임종인(2002)

〈표 8〉 분석대상에 따른 분류기준

구분	세부 항목 설명
디스크 포렌식	물리적 저장장치인 하드디스크, 플로피디스크, DVD, CD-ROM 등 각종 보조기억장치에서 증거를 수집/분석하는 기술분야
네트워크 포렌식	네트워크 정보(Network Traffic Flows)와 전송 데이터(Contents)를 수집하여 필요한 증거를 추출하고 분석하여 보고하는 과정을 연구하는 기술분야
시스템 포렌식	컴퓨터의 운영체제(Windows, Macintosh, LINUX, ZENIX 등), 응용 프로그램 및 프로세스를 분석하여 증거를 확보를 연구하는 기술분야
모바일 포렌식	전자수첩, 휴대폰, 캠코더, PDA, 디지털 카메라, MP3 Player, 메모리카드 등 휴대용 기기에서 필요한 정보를 입수하여 분석을 연구하는 기술분야
인터넷 포렌식	인터넷으로 서비스되는 월드와이드웹(WWW), FTP, USENET 등 인터넷 응용 프로토콜을 사용하는 분야에서 증거를 수집을 연구하는 기술분야
데이터베이스 포렌식	데이터베이스로부터 데이터를 추출 · 분석하여 증거를 획득을 연구하는 기술분야 (기업의 분식회계, 탈세, 횡령 등의 수사 시, 대상 기업의 시스템에 저장되어 있는 데이터베이스 분석 등)

출처 : 이형우 외(2002)

〈표 9〉 법률 적용분야에 따른 분류기준

구분	세부 항목 설명
민사	개인 대상 사적인 법무 관련 연구
형사	형법의 적용을 받는 법무 관련 연구
감사	법원의 개입 없이 관련 정보를 요청에 의해 공개 관련 연구 (회계, 내부 감사)

포렌식(System Forensic), 인터넷 포렌식(Internet Forensic), 데이터베이스 포렌식(Database Forensic)으로 분류하였다. 이에 대한 세부 설명은 〈표 8〉과 같다.

(7) 법률적용 분야

디지털 포렌식은 디지털 자료가 법적 효력을 갖도록 만드는 과정이기에, 법적 효력을 갖고 어떤 법률 분야에 적용할 수 있는지에 대한 연구를 추가적으로 실시하였다. 법률 적용분야와 관련하여 민사, 형사, 감사로 분류기준을 정하였으며, 저자의 소속은 공공, 민간, 학계로 나누었다. 각 세부 분류 및 정의는 〈표 9〉와 같다.

Ⅳ. 연구 분석 결과

1. 선행 연구현황

본 연구는 2007년부터 2016년까지 한국연구재단 등재지 등재후보지에 게재된 디지털 포렌식 관련 연구 총 239편을 대상으로 진행하였다. 〈표 10〉에서 볼 수 있는 바와 같이 10년간 총 38종의 학술지에 관련 논문이 게재되었다. 특히, '정보보호학회 논문지'에 총 88편(36.8%)으로 가장 많은 논문이 게재되었으며, 디지털 포렌식 연구는 최근 5년 사이 18편이 게재되며 10년간 총 26편(10.9%), 한국컴퓨터정보보호학회 논문지에 총 17편(7.1%)의 논문이 게재되어 전체 50% 이상의 분포를 보이고 있어, 전체적으로 정보통신분야에서 디지털 포렌식 관련 연구가 많이 게재되고 있음을 확인할 수 있다. 이는 디지털 기기를 분석대상으로 하는 미디어적 특성 때문인 것으로 판단된다.

2. 분석결과

1) 연구주제

디지털 포렌식 관련 연구를 연구주제 측면에서 분류한 결과, 〈표 11〉과 같이 기술관련 연구가 156편(65.3%)으로 과반수를 차지하였다. 기술 관련 연구의 비중은 꾸준히 높게 나타나고 있긴 하지만, 디지털 포렌식의 도메인, 분석절차, 관련 적용 법률 등에 대한 연구의 비

〈표 10〉 게재 논문지별 분포

저널명	07년~11년	12년~16년	계
정보보호학회논문지	37 (35.2)	51 (38.1)	88 (36.8)
디지털 포렌식연구	8 (7.6)	18 (13.4)	26 (10.9)
한국컴퓨터정보보호학회논문지	15 (14.3)	2 (1.5)	17 (7.1)
한국정보통신학회	2 (1.9)	10 (7.5)	12 (5.0)
정보과학회논문지	4 (3.8)	6 (4.5)	10 (4.2)
기타	39 (37.2)	47 (35)	86 (36)
계	105	134	239

율이 점차 증가함에 따라 그 비율이 68.6%에서 62.7%로 상대적으로 줄어들었음을 확인할 수 있다.

2) 연구방법론

디지털 포렌식 관련 연구의 연구방법으로는 특정 포렌식 분야에 대한 내용분석을 통해 개념을 확립하는 개념연구를 활용한 연구의 빈도가 가장 높게 확인되었다(104편, 43.5%). 이는 새롭게 등장하는 분석대상과 분석 방법에 대해 정의하는 연구가 계속되었기 때문이다. 이어 도구개발(75편, 31.4%), 시스템평가(59편, 24.7%) 등 특정 분석 대상 및 환경에서 활용 가능한 기술을 개발하고 검증하는 연구가 그 다음으로 많이 적용되고 있음을 확인하였다. 기존 IS 분야의 연구에서 많이 활용되는 설문이나, 연구 분야 전반에 대한 동향 파악을 위한 메타스터디는 아직 진행비율이 낮게 확인되었다.

3) 분석단위

〈표 13〉과 같이, 분석단위 측면에서는 기술단위의

〈표 11 〉 연구주제별 분포

단위 : 명 (%)

구분	07년~11년	12년~16년	계
기술	72 (68.6)	84 (62.7)	156 (65.3)
도메인	14 (13.3)	21 (15.7)	35 (14.6)
절차	10 (9.5)	17 (12.7)	27 (11.3)
법률연구	6 (5.7)	10 (7.5)	16 (6.7)
기타	3 (2.0)	2 (1.5)	5 (2.1)
계	105	134	239

〈표 12〉 연구방법별 분포

단위 : 명 (%)

구분	07년~11년	12년~16년	계
개념연구	44 (41.9)	60 (44.8)	104 (43.5)
도구개발	34 (32.4)	41 (30.6)	75 (31.4)
시스템평가	27 (25.7)	32 (23.9)	59 (24.7)
설문	0 (0.0)	1 (0.7)	1 (0.4)
계	105	134	239

〈표 13〉 분석단위별 분포

단위 : 명 (%)

구분	07년~11년	12년~16년	계
기술	78 (74.3)	95 (70.9)	173 (72.4)
개인	3 (2.9)	15 (11.2)	18 (7.5)
국가	6 (5.7)	4 (3.0)	10 (4.2)
그룹	1 (1.0)	1 (0.7)	2 (0.8)
기타	17 (16.2)	19 (14.2)	36 (15.5)
계	105	134	239

연구가 총 173편으로 전체 연구의 72.4%를 차지하는 것으로 나타났다. 이는 아직 디지털 포렌식 연구에 있어 국가, 조직, 개인에의 적용이나 활용을 다루는 연구보다는 특정 분석대상이나 기술에 초점을 맞춘 연구 위주였음을 짐작할 수 있다.

4) 연구자 소속

저자의 소속 측면에서는 〈표 14〉에서 볼 수 있듯, 저자가 학계 소속인 경우가 160편(66.9%)으로 가장 많이 나타나 지금까지 학계 주도의 연구가 활발히 진행되었음을 알 수 있다. 뒤이어 공공부문 소속 저자의 경우가 37편(15.5%), 민간기업 소속인 경우가 3편(1.3%)로 나타났다.

또한 민,관,학 공동연구는 39편(16.3%)이며, 최근 5년간 연구 비율에서 공공분야 소속 저자의 포렌식 연구 비율(13.3%→17.2%)과 공동연구의 수가 증가(18건→21건)함을 볼 수 있는데, 이는 최근 실무의 이슈를 반영한 연구에 대한 니즈가 높아지고 있음을 생각할 수 있다.

5) 디지털 포렌식 절차

디지털 포렌식은 크게 디지털 기기의 증거를 복구하고, 복구한 데이터를 수집하여 보관하고 수집한 데이터를 분석하는 단계로 구분할 수 있다. 본 연구에서 분석단계 측면에서 분석한 결과, 〈표 15〉와 같이 증거수집단계의 연구가 88편(36.8%), 포렌식 전반의 절차에 대한 연구가 61편(25.5%), 증거분석단계의 연구가 57편(23.8%), 증거복구단계의 연구가 26편(10.9%), 수집과 분석단계를 함께 다루는 연구가 4편(1.7%)으로 나타났다. 디지털 포렌식의 특정 단계에 대한 연구가 많이 수행되고 있지만, 포렌식 분석 전반에 관한 연구도 다수 진행된 것을 확인할 수 있었는데, 이는 새로운 분석대상의 등장과, 분석기술을 도입하는 경우, 이에 대한 분석 절차를 새롭게 정의하고 전체적으로 조망하기 위한 연구가 꾸준히 진행되고 있기 때문으로 볼 수 있다.

〈표 14〉 저자소속별 분포

단위 : 명 (%)

구분	07년~11년	12년~16년	계
학계	71 (67.6)	89 (66.4)	160 (66.9)
합동	18 (17.1)	21 (15.7)	39 (16.3)
공공	14 (13.3)	23 (17.2)	37 (15.5)
민간	2 (1.9)	1 (0.7)	3 (1.3)
계	105	134	239

〈표 15〉 분석단계별 분포

단위 : 명 (%)

구분	07년~11년	12년~16년	계
증거수집	43 (41.0)	45 (33.6)	88 (36.8)
포렌식전반	29 (27.6)	32 (23.9)	61 (25.5)
증거분석	23 (21.9)	34 (25.4)	57 (23.8)
증거복구	8 (7.6)	18 (13.4)	26 (10.9)
수집+분석	2 (1.9)	2 (1.5)	4 (1.7)
기타	0	3 (2.2)	3 (1.3)
계	105	134	239

6) 디지털 포렌식 대상매체 및 기술

디지털 포렌식은 증거의 수집, 분석을 진행하는 대상에 따라 크게 서버, PC등 컴퓨터에 대한 분석을 하는 호스트 기반 포렌식과 네트워크상의 정보를 수집, 분석하는 네트워크 기반 포렌식으로 구분할 수 있으며(김혁준 외, 2008) 세부 분석 대상에 따라 〈표 16〉과 같이 구분할 수 있다. 이 중 컴퓨터 운영체제, 운영프로그램 및 프로세스를 분석하는 시스템 포렌식에 대한 연구가 50편(20.9%), 물리적 저장장치에 대한 분석인 디스크 포렌식 연구가 48편(20.1%), 휴대용 기기에 대한 분석인 모바일 포렌식 연구가 31편(13%), 인터넷 응용프로토콜을 사용하여 증거를 수집 분석하는 인터넷 포렌식이 21편(8.8%), 네트워크 포렌식이 17편(7.1%), 데이터베이스 포렌식이 12편(5%)으로 나타났다. 이 중 시스템 포렌식(24.8%→17.9%)과 네트워크 포렌식(13.3%→2.2%) 분야는 최근 그 연구 비율이 줄어들고 있는 것으로 확인되었고, 디스크포렌식(15.2%→23.9%)과 인터넷 포렌식(4.8%→11.9%) 분야의 연구는 비율이 크게 늘어난 것으로 확인되었다.

7) 법률적용 분야

디지털 포렌식은 디지털 데이터를 체계적인 절차에 따라 수집, 분석하여 법적 효력을 갖게 하려는 목적으로 수행된다. 법적 효력을 갖은 데이터를 수사 분야의 어떤 분야에 활용하는지에 따른 구분을 〈표 17〉과 같이 살펴보면, 형사 사건 관련 연구가 67편(28%), 민사 사건 관련 연구가 26편(10.9%), 기업 감사 관련 연구가 5편(2.1%)로 나타났다. 반면 특정 기기나 분석 기술 관련 연구 등의 법적 효력 및 적용 수사 분야 확인이 어려운 연구가 141편(59%)으로 과반 이상으로 나타났다.

Ⅴ. 연구 요약 및 시사점

〈표 16〉 세부 분석대상별 분포

단위 : 명 (%)

구분	07년~11년	12년~16년	계
기타 디지털 디바이스	26 (24.8)	34 (24.3)	60 (25.1)
시스템	26 (24.8)	24 (17.9)	50 (20.9)
디스크	16 (15.2)	32 (23.9)	48 (20.1)
모바일	14 (13.3)	17 (12.7)	31 (13.0)
인터넷	5 (4.8)	16 (11.9)	21 (8.8)
네트워크	14 (13.3)	3 (2.2)	17 (7.1)
데이터베이스	4 (3.8)	8 (6.0)	12 (5.0)
계	105	134	239

〈표 17〉 적용 수사분야별 분포

단위 : 명 (%)

구분	07년~11년	12년~16년	계
형사	20 (19.0)	47 (35.1)	67 (28.0)
민사	6 (5.7)	20 (14.9)	26 (10.9)
감사	4 (3.8)	1 (0.7)	5 (2.1)
기타	75 (71.4)	66 (49.3)	141 (59.0)
계	105	134	239

본 연구는 국내 디지털 포렌식 분야의 연구 동향을 살펴보고, 추후 해당 분야의 연구 방향과 시사점을 도출하고자 2007년부터 2016년까지의 국내 등재지 및 디지털포렌식 관련 등재후보지에 게재된 논문 239편을 대상으로 연구주제, 연구방법, 분석단위, 연구자의 소속, 디지털 포렌식의 분석절차, 디지털 포렌식 대상 매체 및 기술, 법률 적용 분야 측면에서 분석하였다.

연구 주제 측면에서는 데이터 수집과 분석 기술 관련 연구의 비중이 높지만, 그 연구 비중은 점차 줄어들고 있는 것으로 확인되었으며, 타 주제의 연구가 비중이 점차 높아지고 있는 것으로 나타났다. 이는 지금까지 다수의 연구가 분석 대상 기기에 따른 데이터 수집 기술과 분석 기술을 파악하는데 집중되어 있었기 때문으로 판단된다. 이러한 결과는 해외 연구동향과 일치하는 경향을 보이고 있으며, 특히 이로 인해 국내 디지털 포렌식 관련 하드웨어 기술 수준은 글로벌 기술력을 주도하고 있다. 따라서 향후 파일 카빙을 위한 소프트웨어적인 알고리즘 설계와 관련된 기술 개발 등도 필요할 것으로 예상된다.

디지털 포렌식 분야가 성장함에 따라 적용 기술 뿐 아니라 디지털 포렌식을 적용하기 위한 관련 법률이나 제도적 분석에 대한 내용, 포렌식 담당 인력의 양성이나 업무효율 증진 방안 등 수행 환경에 대한 연구 역시 필요가 점차 증가할 것이며, 해당 분야에 대한 연구 비중 역시 높아질 것으로 보인다.

연구 방법 측면에서는 개념연구에 대한 빈도가 가장 높게 나타났다. 이는 디지털 포렌식은 분석 대상과 분석 기술이 빠르게 확산되고 있는 분야이기에, 새로운 적용 대상과 기술에 대한 정의와 개념 확립이 계속적으로 진행되고 있기 때문으로 볼 수 있다. 반면 그 외의 연구가 특정 분석 대상 및 기술의 개발 및 검증하기 위한 도구개발, 시스템평가에 국한되어 진행되었다는 결과는 지금까지의 디지털 포렌식 연구가 기술적인 측면에만 집중되어 진행되었다는 연구주제 측면의 결과와 상통한다. 디지털 포렌식은 단지 분석 대상이나 기술에만 국한된 것이 아닌 다양한 분야가 융합된 분야이기에, 공학적 방식에서의 접근을 넘어 제도적, 정책적, 환경적 측면에 대한 접근이 있어야만 분야의 실무적 성격을 반영할 수 있을 것이다. 또한 추후 실무 적용과 관련한 다양한 측면의 연구 주제를 도입한다면, 사회과학 연구에서 활용되는 다양한 연구방법을 디지털 포렌식 관련 연구에 적용할 수 있을 것이다.

연구자의 소속 측면에서는 과거 학계 소속 연구자의 연구 비율이 압도적이었지만 최근 연구자의 소속이 공공 연구기관이나 실무 담당기관인 비율이 증가하고 있다. 이는 학술 연구에 현장의 이슈를 반영하기 위한 수사관련 기관이나 민간기업의 니즈가 반영된 것이라 추정할 수 있다. 디지털 포렌식 분야는 수사 현장에서 디지털 증거의 법적 효력을 확보하기 위한 증거 수집과 분석과 관련한 연구이기에 매우 실무적인 분야이기에, 현장을 반영하지 않은 이론적이고 개념적인 연구는 한계를 지닌다. 최근 디지털 포렌식 업무 실무자의 역량 강화를 위한 특별 교육 과정 개설이 증가하고, 이를 통해 학계와 디지털 포렌식 실무기관 간의 유기적 협력이 증가하고 있다. 이처럼 공공, 혹은 실무기관 소속 연구자의 연구비율의 증가는 실무적 연구 활성화와 연구 주제의 다양성 측면에서 매우 고무적이라 할 수 있다.

디지털 포렌식의 분석 절차 측면에서는 지금까지는 포렌식 전반에 대한 연구의 비중이 높았음을 확인할 수 있는데, 이는 새롭게 등장하는 분석 대상과 새로이 개발된 분석기술을 적용한 분석 프로세스 전체를 정의하기 위한 연구가 많이 진행되었기 때문임을 알 수 있다. 특정 분석 단계에 대한 연구에서는 증거 수집과 분석 단계에 대한 연구의 비중에 비해 증거 복구 단계에 대한 연구는 상대적으로 적게 진행된 것을 볼 수 있었다. 지금까지는 증거를 수집하고 분석하기 위한 기술을 개발에 치중해 왔으나, 포렌식 기술이 고도화됨에 따라 디지털 정보의 분석을 피하는 목적의 안티포렌식 기술 역시 발달하고 있다. 따라서 이에 대응하기 위한 증거 분석 관련 연구는 아직까지는 많이 수행되지 않았지만 앞으로 그 비중이 증가할 것으로 예상할 수 있을 것이다.

디지털 포렌식 대상 매체 및 기술 측면에서는 시스템

포렌식, 네트워크 포렌식의 연구 비율은 최근 5년 사이 많이 줄어든 반면, 인터넷 포렌식과 기타 디지털 디바이스 관련 포렌식 연구의 비율이 높아진 것을 확인할 수 있었다. 이는 개인의 디지털 디바이스의 사용과 인터넷 사용의 증가로 인해 사이버 범죄와 연관될 환경에 더욱 높은 비율로 노출되기 때문에 나타난 결과라고 볼 수 있다. 분석단위 측면에서 개인을 대상으로 한 연구의 비율이 최근 높아지고 있는 것과 법률 적용 분야 중 민사 관련 연구의 비율이 높아지는 것도 이와 같은 맥락으로 볼 수 있을 것이다.

대상 기술과 관련하여 살펴보면 디지털 데이터가 점점 대용량화 되고 있으므로 포렌식 이미징을 만드는 과정의 고속화와 여러 포렌식 툴 간 호환성을 위한 포렌식 이미지 포맷에 대한 표준화 관련 연구에 관심이 집중되고 있는 추세이다. 이는 해외 연구 분야에서도 동일하게 나타나고 있는데, 대용량 데이터 처리를 위한 알고리즘 설계에 관한 연구들과 크게 다르지 않다.

마지막으로 지금까지 국내에서의 디지털 포렌식은 민·형사 소송에서 법정의 증거로 활용되기 위한 증거로써 활용되어 왔으나, 디지털 포렌식 기술은 인터넷 관련 범죄 뿐 아니라 기업의 사내 보안 누출과 네트워크 침입, SNS 내의 개인정보 유출, 사물인터넷, 핀테크 등의 환경에 활용되는 등 그 활용 범위가 확대되고 있으며, 민간 기업들의 본격적 시장진출을 통해 시장이 활성화 되고 있다. 국내에서는 현장에서 법무부 산하의 유관기관과 민간업체 간의 상호협력을 통해 인프라를 구축하고, 빠르게 변하는 환경의 변화에 대응하기 위해 관련 기술의 개발을 장려하고, 특허권을 확보할 필요가 높아지고 있다.

분석 결과와 국내 디지털 포렌식 분야에서 보이는 이슈를 바탕으로 추후 연구방향에 대해 다음과 같이 몇 가지 제안을 하고자 한다.

첫째, 디지털 포렌식의 연구 주제 및 분석 대상을 기술에서 더욱 확장시킬 필요가 있다. 지금까지의 연구는 분석 대상 및 분석 도구에 대한 컴퓨팅적 내용에 초점을 두고 수행되었다. 하지만 디지털 포렌식은 단순히 기술에 국한되지 않고 수집 분석한 디지털 증거가 법적인 증거를 갖도록 하는 일련의 과정을 의미한다. 과정에서 활용하는 도구에 대한 기술적 관점을 넘어, 절차의 효율성 향상을 위한 수행 인력이나 조직 운영 관점의 연구도 가능하다. 또한 개인이나 조직 관점에서 발생할 수 있는 법적 문제 이슈에 초점을 둔 연구, 디지털 범죄에 대한 개인이나 조직의 사전 대응방안 등 사회 전반을 대상으로 연구 범위를 확장할 수 있을 것이다. 또한 이를 수행하는데 사회과학분야에서 활용되는 설문, 사례연구 등 다양한 연구 방법을 활용할 수 있을 것이다.

둘째, 지금까지의 학계 주도의 연구에서 민간과 공공 참여 연구의 확대가 필요하다. 디지털 포렌식 분야는 인터넷 기술 발달로 인한 사회적 요구가 높은 실용적 학문이다. 이를 위해서는 컴퓨터 분야를 기반으로 법률, 심리학, 법의학 등 다양한 학문이 포괄적으로 융합되어야 하며, 경찰의 사이버 범죄 담당인력, 기업의 정보시스템 담당자 혹은 디지털 포렌식 분석을 위한 도구 개발 인력 등의 공동 연구를 통해 현장의 이슈 반영하여 실무적이고 실용적인 연구를 수행해야 한다.

마지막으로 개인 차원의 디지털 포렌식에 대한 연구가 더욱 수행되어야 할 것이다. 기술의 발달에 따라 개인이 사용하는 디지털 디바이스의 수는 양적으로 증가하고 있으며, 그만큼 개인이 디지털 범죄에 노출되는 위험 역시 증가하고 있다. SNS 사용의 증가로 인해 개인 프라이버시의 유출, 디지털 저작권의 보호 등의 이슈는 계속 커지고 있지만, 이에 대한 개인의 대응이나 보호를 위한 디지털 포렌식 관점의 연구는 아직 많이 부족한 것(7.5%)으로 확인되었다. 따라서 국가적 이슈나 기업 대상을 분석단위로 하는 연구뿐 아니라 개인 대상의 연구에 대한 관심이 요구된다.

이와 같이 디지털 포렌식 분야에 의미 있는 시사점을 도출하였음에도 불구하고, 본 연구는 몇 가지 한계점을 가지고 있다. 우선 본 연구에서는 IS분야에서 사용한 기존의 대표적인 분석 관점에 실무적 관점을 추가하여 분석을 진행하고 이를 토대로 시사점을 도출하였다. 하

지만 디지털 포렌식은 기술과 사회과학적 요소를 모두 갖춘 분야이기에 IS분야의 분석 관점 이외에 다양한 관점의 분석이 가능할 것으로 예상한다. 추후 공학적 관점 등 다른 학문 분야에서 사용한 분류체계를 추가하여 수행한다면 새로운 각도에서의 시사점을 도출할 수 있을 것이다.

또한, 본 연구는 2007년부터 2016년까지 지난 10년간의 논문으로 한정하였으며, 5년 단위의 분석을 수행하였다. 한정적인 연구기간으로 인해 데이터베이스 용량의 증가, 인터넷 속도 향상, 개인 모바일 디바이스의 확산 등 시대적 이슈에 따른 변화를 파악하기에 한계가 있었다. 추후 2007년 이전의 논문과 특이 수치가 나타나는 연도의 이슈에 대해 복합적으로 분석한다면 관련 기술, 트렌드의 변화를 볼 수 있는 폭넓은 분석을 통해 더 많은 시사점을 제공할 수 있을 것이다.

마지막으로 본 연구에서 간략하게 해외 디지털 포렌식 연구 현황에 대해 정리하긴 하였지만, 본 연구의 주제가 국내 연구 동향을 기반으로 향후 연구 방향을 제시하는데 그 목적이 있는바 분석 기준 및 내용을 매우 간략하게 서술되었다. 하지만 추후 연구에서 본 연구에서 활용한 분석 관점과 동일하게 해외 디지털 포렌식 연구 동향에 대해 분석하고 본 연구의 내용과 비교한다면, 더욱 많은 논의를 이끌어 낼 수 있을 것으로 예상한다.

■ 참고문헌

경찰청 사이버안전국 (2016). “전체사이버범죄 발생 검거 현황.” http://cyberbureau.police.go.kr/share/sub3.jsp?mid=030300

김혁준·이상진 (2008). “분석 사례를 통해 본 네트워크 포렌식의 동향과 기술.” 「정보보호학회지」, 18(1): 41-48.

신용태 (2006). 「디지털증거의 무결성 유지를 위한 절차와 시설에 관한 연구」. 대검찰청.

양근원 (2006). “디지털 포렌식과 법적 문제 고찰.” 「형사정책연구」, 17(2): 207-248.

연규철·김문호·김도현·이상진 (2016). “스마트 기기에 설치된 내비게이션 어플리세이션의 위치 정보 흔적 연구.” 「정보보호학회논문지」, 26(1): 109-115.

윤신자·이상진 (2013). “전자정보의 압수 수색 절차 개선 방안 연구 - 국가안보사건을 중심으로-.” 「경찰학연구」, 13(4): 227-252.

윤종철·박용석 (2016). “KakaoTalk의 채팅 메시지 포렌식 분석 연구 및 WhatsApp의 Artifacts 와의 비교 분석.” 「한국정보통신학회논문지」, 20(4): 777-785.

이경식 (2016). “맥 포렌식을 통한 아이폰 아티팩트 분석 기법.” 「정보보호학회지」, 26(5): 17-21.

이대명 (2016). “토픽브리핑 - 대해킹시대 사이버범죄가 증가하는 이유.” http://www.itworld.co.kr/news/99229.「IT WORLD」, 5월 13일.

이상복 (2008). “디지털 포렌식 업무의 법·제도적인 개선 방향.” 「서강법학연구」, 10(2): 139-178.

이영주·강경희·이중정·신재우 (2010). “한국의 전자정부 연구 동향 분석-국내 학술지 게재 논문을 중심으로.” 「정보화정책」, 17(3): 36-56.

이형우·이상진·임종인 (2002). “컴퓨터 포렌식스 기술.” 「정보보호학회지」, 12(5): 8-16.

장성민·박정흠·박찬웅·이상진 (2015). “Full Disk Encryption 환경에서 디지털 증거 수집 절차에 관한 연구.” 「정보보호학회논문지」, 25(1): 39-48.

전상덕·한기준·홍동숙 (2006). “디지털 포렌식의 기술 동향과 전망.” 「정보화정책」, 13(4): 3-19.

주정민·나형진 (2015). “사물인터넷(IoT)에 관한 국내 연구 동향 분석.” 「정보화정책」, 22(3): 3-15.

탁희성 (2008). “디지털 증거의 신뢰성 확보의 전제로서 디지털 포렌식에 대한 소고.” 「경찰학논총」, 3(1): 173-198.

한국과학기술정보연구원 (2014). 「Market Report : 법과학(Forensic science) 감식 제품 및 서비스 – 국내 민간 시장 활성화 통한 성장기대」. 서울: 한국과학기술정보연구원

한국과학기술정보연구원 (2016). 「Market Report : 디지털 포렌식 - 정부 유관기관들의 적극적 협조가 필요」. 서울: 한국과학기술정보연구원

한국정보보호진흥원 (2003). 「라우터 보안관리 가이드」. 서울: 한국정보보호진흥원

Credence Research (2016). 「Digital Forensics Market By Type (Computer Forensics, Mobile Devices Forensics, Cloud Forensics), By Service (Digital Investigation And Consulting Services, Incident

Response, System Integrators, Training And Certification, Support And Maintenance) – Growth, Share, Opportunities & Competitive Analysis, 2016 – 2023」. Credence research

David Lillis, Brett Becker, Tadhg O'Sullivan & Mark Scanlon (2016). "Current challenges and future research areas for Digital Forensic investigation", Annual ADFSL Conference on Digital Forensics, Security and Law.

Globe Newswire (2015). 「Digital Forensics Need to cooperate with government agencies」. Newswire

Stephenson, P. (2003). A comprehensive approach to digital incident investigation. Elsevier.

Symantec (2016). *Internet Security Threat Report*, 5–7. Symantec

Iris Vessey, V. Ramesh & Robert L. Glass (2002). "Research in Information Systems: An Empirical Study of Diversity in the Discipline and Its Journals." *Journal of Management Information Systems*, 19(2): 129–174.