

국내 디지털 포렌식 분야에서 법률적 이슈사항의 중요도 인식에 따른 우선순위 비교 연구

A Study for Comparing the Legal Importance of Digital Forensics Issues in Korea

이 재 빈 (Jae Bin Lee)

안랩

성 원 경 (Won Kyung Sung)

연세대학교 정보대학원

이 중 정 (Choong C. Lee)

연세대학교 정보대학원 교수, 교신저자

요 약

현대사회, 범죄에 관련된 많은 기록들이 디지털 상에 남겨지고 있다. 디지털 정보는 원본구분이 어렵고, 위·변조가 용이한 특징을 가지고 있기 때문에 과학적 수사기법을 통해 증거요건을 갖추도록 하는 디지털 포렌식의 중요성이 커지고 있다. 하지만 현재 디지털 포렌식 기술은 빠른 변화, 국가 경계의 모호함 등으로 증거수집 절차나 도구 오류 등에서 많은 비효율성을 보유하고 있다. 따라서 본 연구는 국내 디지털 포렌식 이슈의 우선순위 도출을 위하여 호주의 Brungs-Jamieson 연구에서 도출한 17가지 디지털 포렌식 분야의 이슈를 국내 상황에 맞게 재정의 후, 디지털 포렌식 전문가들에게 이슈 별 중요성 및 우선순위 조사 인터뷰를 실시하였다. 인터뷰는 경찰, 정부 및 공기업, 민간기업, 그리고 법조계 그룹으로 나누어 진행되었으며, 이를 통해, 기존의 호주, 미국과의 비교분석뿐만 아니라, 국내의 각 그룹별 조사결과의 차이를 비교 분석할 수 있었다. 연구 결과로서 국내 디지털 포렌식 분야에서의 주요 핵심 이슈사항은 ‘모범 사례 지침과 표준의 중요성’으로 도출되었으며 법률적 이슈사항에 대해 세 그룹으로 분류하여 그룹 간 차이를 확인할 수 있었다. 이를 통해 그룹, 국가 간 이슈의 우선순위 및 중요도 차이 원인에 대해 파악할 수 있었으며 향후 국내 디지털 포렌식 분야 발전을 위해 그룹 별 우선 해결 사항들을 제시할 수 있을 것으로 기대한다.

키워드 : 디지털 포렌식, 우선순위, 법률적 이슈사항, 중요도

I. 서 론

1.1 연구배경

현대 사회의 급격한 발전에 따라 컴퓨터, 그리고 모바일은 현대 사회의 필수 요소가 되었다. 대다

수의 기업들의 생산성 향상을 위한 도입을 시작으로, 개인의 PC 그리고 스마트폰과 같은 모바일 까지, 정보시스템은 급진적으로 확산되어 왔다. 하지만 정보시스템의 발전과 증가만큼, 보안 인식 및 기술은 이를 따라가지 못하면서 사이버 범죄의 발생 역시 증가하고 있다(권영욱, 2007). 한국

경제의 “사이버 범죄 10년새 90% 증가” 기사를 보면 2004년 약 7만 7천 건이던 사이버 범죄는 2015년 약 14만 5천 건으로 10년간 약 76.7% 급증한 것을 알 수 있으며, 이는 같은 기간 전체 범죄 건수가 5.4% 감소한 것과 비교해 보았을 때 매우 대조적임을 알 수 있다. 또한 사이버 범죄가 아닌 강력, 및 지능범죄를 해결하기 위한 증거로서 디지털 기기들이 사용되는 경우 역시 크게 늘었는데, 연합뉴스의 “부산 범죄수사에 디지털 증거 분석 의뢰 급증” 기사에 따르면 부산 경찰청의 디지털 포렌식 팀의 2012년 증거분석 사건 의뢰 건수는 513건으로 2011년 364건에 비해 41% 증가하였으며, 그 중 절도와 성폭력 등 강력사범이 241건, 사기, 뇌물 등 지능사범이 152건, 인터넷 사범 29건으로서, 이를 통해, 디지털 증거들은 사건의 종류에 구애 받지 않고 모든 범죄사실을 규명 하는 데에서 매우 중요한 역할을 하고 있는 것을 알 수 있다. 하지만 디지털 정보는 원본과 복사본의 구분이 어렵고, 위·변조가 용이하다는 특징 때문에 증거로 채택이 어렵다는 문제점을 보유하고 있다. 따라서 디지털 정보가 법적 증거로서의 효력이 있기 위해서는 정보의 수집·보존·처리 전 과정에 과학적 수사기법을 통해 증거의 요건을 갖추는 특별한 절차와 방법을 필요로 하는데 이런 일련의 과정을 디지털 포렌식이라 한다(대검찰청, 2006).

이렇게 디지털 포렌식은 컴퓨터, 모바일과 같은 장치에서, 합법적이고 표준적인 방법을 통해 필요한 디지털 증거를 법적 소송 절차에 제공하는, 현대 사회에서 점점 중요성이 증가하고 있는 분야라고 할 수 있다. 또한, 디지털 포렌식 분야의 수요 역시도 급증하면서, 법률 프로세스, 역할, 사법권 이용 범정 절차, 증거 분석 및 제출 등 전반적인 절차에서도 좀 더 효율적인 대응을 요구 받고 있다(Brungs and Jamieson, 2005). 따라서 각 기관들은 이러한 문제들을 해결하기 위해 기술, 정책, 제도, 법 등 다양한 부분에서 노력을 이루고 있지만 디지털 포렌식이 형성된 지 오래되지 않았다는

점, 기술의 빠른 변화로 인한 다양성 증가한다는 점, 그로 인해 연계되는 사항에서 새로 형성되는 문제점 등 상호 연계되는 문제점이 증가하여 이에 대한 해결이 매우 어려운 상황이다. 대표적인 예로, 인터넷의 본질적 특성인 국가 경계의 모호함으로 인한 국가간 관할권 경계와 정보수집의 제한 문제(Broadhurst, 2006; Conley and Bryan, 1999; Liles *et al.*, 2009; Pocar, 2004; Reid, 2006), 디지털 범죄 증거수집 절차를 위한 도구의 오류율과 일관성, 표준화 문제(Carney and Rogers, 2004; Meyers and Rogers, 2004; Reith *et al.*, 2002), 그리고 비전문가도 쉽게 이해할 수 있어야 한다는 디지털 증거의 명확성과, 이해 가능성에 대한 이슈(Broucek and Turner, 2002; Carney and Rogers, 2004; Laubscher *et al.*, 2005; Witter, 2001) 등을 들 수 있다.

위에 언급된 이슈들 외에도 디지털 포렌식 분야에서는 여러 이슈들이 존재해 왔다. 따라서 해결의 필요성을 느낀 호주에서는 2003년에 디지털 포렌식 전문가 포럼을 열어 브레인스토밍과 토론을 통해 17가지 법률적 핵심이슈들을 도출하였다. 하지만 해당 17가지 핵심 이슈들을 한 번에 해결하기에는 자원의 한정성 및 이해관계자 문제들이 있었고, 이를 해결하기 위하여 호주와 미국에서는 각각 2003년, 2007년, 해당 핵심이슈에 대해 중요도를 조사하여 우선순위를 도출하게 되었다. 동일한 이슈에 대한 두 국가에서의 설문 결과들은 디지털 포렌식 발전을 위한 효율적인 자원 활용과 거버넌스를 확보에, 그리고 일반적인 전세계적 공통 이슈 도출에 도움을 주었다. 따라서 국내에서도 디지털 포렌식 분야에서 핵심 이슈사항들에 대해 조사 후 해당 결과를 비교분석 할 필요가 있다고 여겨지게 되었다. 따라서 해당 연구에서는 기존 호주 디지털 포렌식 전문가들이 도출한 17가지 디지털 포렌식 분야의 이슈를 국내 상황에 맞게 재정의 후, 디지털 포렌식 전문가들에게 이슈 별 중요성과 이슈 간 우선순위 조사를 실시하였다. 조사는 경찰, 정부 및 공기업, 민간기업, 그리고 법조계 그룹으로 나누어 진행되었으며,

이를 통해, 기존의 호주, 미국과의 비교 분석뿐만 아니라, 국내의 각 그룹별 조사결과와의 차이를 비교 분석할 수 있었다. 이를 통하여 그룹, 국가 간 이슈에 대한 우선순위 및 중요도의 차이가 오는 원인에 대해 파악 할 수 있었으며 향후 디지털 포렌식 분야가 발전하기 위해 우선적으로 해결해야 할 사항들을 제시하였다.

II. 문헌 연구

2.1 디지털 포렌식의 정의

포렌식의 사전적 의미는 ‘법정의’ 또는 법과학의’라는 뜻으로써 법정에서 증거를 사용하기 위해 증거를 수집·보존·처리시 과학적·기술적인 기법을 사용하여 증거가치가 상실되지 않도록 하는 일련의 절차 내지 과정을 의미한다(탁희성 등, 2006). 기존의 포렌식은 범의학 분야 내 DNA 감식, 변사체 감시 등에 사용 되었으나 컴퓨터 범죄의 증가와 함께 해당 범죄에 대한 증거 확보를 위한 분야인 컴퓨터 포렌식이 생겨나게 되었다. 초창기 컴퓨터 포렌식은 컴퓨터 중심 증거 확보에 중점을 두고 있었으나, 점차 증거를 포함하고 있는 본 요소인 디지털 장비로 초점이 이동하며 컴퓨터 포렌식에서 디지털 포렌식으로 변화하게 되었다(탁희성 등, 2006). 오늘날의 디지털 포렌식은 단순히 컴퓨터에서 발생한 범죄의 증거 수집뿐만 아니라 모든 분야의 범죄 증거 수집과정에서 합법적이고 과학적인 범죄 입증절차를 제시하여 범죄를 증명하는 데 기여하고 있다. 따라서 디지털 포렌식은 단순히 디지털 증거 수사를 위한 과학적인 방법 및 절차임과 동시에 디지털 증거를 증거로써의 의미를 부여하는 소송법적 영역의 한 분야이기도 하다(곽병선, 2011). 이러한 디지털 포렌식은 디바이스의 영역, 그리고 디지털 기술에 따라 여러 가지 종류로 나뉘어진다. 먼저, 비 휘발성 물리 저장장치인 하드디스크, USB 등과 같은 보조 기억장치로부터 디지털 증거를 수집하

고 분석하는 디스크 포렌식(전상덕 등, 2006), 네트워크 트래픽 정보와 전송 데이터 내 필요한 증거를 추출하고 분석하여 보고하는 네트워크 포렌식(박종성 등, 2004), 월드와이드웹(WWW), FTP 등 인터넷 응용 프로토콜을 사용하는 분야에서 디지털 증거를 수집하는 인터넷 포렌식, 데이터 베이스로부터 데이터를 추출·분석하여 디지털 증거를 획득하는 데이터 베이스 포렌식(전상덕 등, 2006), 컴퓨터 운영체제, 프로세스 및 응용 프로그램 분석을 통해 디지털 증거를 확보하는 시스템 포렌식(이상복, 2008), 스마트폰, 디지털 카메라 등 휴대용 기기로부터 디지털 증거를 확보하여 분석하는 모바일 포렌식, 클라우드 환경에서 원격, 가상화, 네트워크 등 종합적인 포렌식 과학을 활용해 법적 효력이 있는 증거물을 생성해내고, 클라우드 서비스 제공업체와의 쌍방소통을 통해 내부 및 외부 수사를 원활하게 하는 클라우드 포렌식(Slay and Schulz, 2014) 등, 기본적인 7가지 종류가 있으며 점차 확장되어 가는 추세이다.

2.2 디지털 포렌식 관련 선행 연구

디지털 포렌식의 기술이 단순 범죄뿐만 아니라 의료, 군사 및 안보, 사회문제 해결 등 다양한 분야에 활용되기 시작하면서 매우 다양한 분야에서 연구가 이루어져 오고 있다(박세환, 2015). 현재 디지털 포렌식은 어카운팅 관련 연구(최재민 등, 2008)나, CCTV 분석 포렌식(김승용 등, 2016)과 같이 기술적 향상을 위한 연구에서부터, 디지털 포렌식의 법률적 고찰이나(권양섭, 2016a) 증거개시 제도와 같은 절차상의 문제(어수용 등, 2016)까지 다양한 관점에서 논의가 되어오고 있으며, 그 영역은 IT의 발전에 맞추어, 과거 컴퓨터에서 인터넷, 클라우드, 모바일, SNS 등으로 확장되어 가고 있다(Chauhan *et al.*, 2016; 어수용 등, 2016; 윤종철 등, 2016).

초기의 디지털 포렌식 분야의 법률 및 절차상의 연구들은 기관의 정책 및, 제도, 법 등에서 다양한

비효율 개선을 위한 디지털 포렌식 수행 절차 개선 관련 이슈들이 대부분이었다(Brungs and Jamieson, 2005; 백승조, 2008). 2003년 17가지 법률적 핵심이슈 및 해당 이슈의 각 부처 별 우선순위를 도출했던 호주 Brungs and Jamieson(2005)의 연구와, 동일 이슈를 대상으로 미국에서 부처별 우선순위를 도출 하였던 Liles(2009)의 연구가 대표적이다. 17가지 동일한 이슈(<표 1> 참조)에 대한 두 국가에서의 연구 결과들은 디지털 포렌식의 효율적인 자원 활용, 거버넌스 확보, 그리고 전 세계적 공통 이슈 도출에 도움을 주었다. 현재의 디지털 포렌식 분야의 법률적 연구들은, 향후 기술로 여겨지는 유비쿼터스나 IOT 관련 포렌식으로까지 그 논의가 확장되어 가고 있는 추세이다(Harbawi and Varol, 2017; 권양섭, 2016b). 하지만 최근 디지털 포렌식의 법률 절차상 연구 동향을 살펴보면, 앞서 언급하였던 최신의 기법들이나 새로운 영역의 이슈뿐만 아니라 ‘수사절차’나, ‘형사절차상의 디지털 증거개시 제도’, 또는 ‘디지털 포렌식 기반의 전자기록물 압수나 이관 절차’ 등과 같은 비교적 초기의 이슈들 역시도 여전히 논의되고 있다는 것을 확인할 수 있다(성혜정 등, 2014; 조광훈, 2014). 이와 같이, 초기에 진행되었던 이슈들이 여전히 논의되는 이유는 몇 가지들을 들 수 있는데, 첫 번째로, 빠른 IT 기술의 발전을 들 수 있다. IT 발전으로 인하여 디바이스의 종류와 영역이 다양화되고 있고, 이로 인하여 포렌식 방법 또한 그 종류와 영역의 개수만큼 다양화하고 복잡해지게 되었다(어수웅 등, 2016). 이는 결국 포렌식의 기술의 전문성과 복잡성을 증가 시켰으며, 해당 이슈는 ‘새로운 포렌식 도구와 기술의 테스트’라는 단순한 이슈에서부터 ‘디바이스에 따라 적용되는 법의 종류’가 다르다는 이슈 그리고 나아가 ‘수사관의 선별요건’, ‘포렌식을 필요로 하는 경찰이나 법조계의 이해도 문제’ 등까지 초기의 이슈들의 논의가 여전히 가능하도록 했다. 두 번째로는, 분석의 주체인 분석관과 수사의 주체인 수사관과의 ‘상호작용의 어려움’을 들 수 있다(신지호, 2016). 디지털 포렌식은 전문적 영역이기 때문에 분석을 수행하는 분

<표 1> Brungs과 Liles 연구의 법률적 이슈사항 명칭

	명칭(호주, 2005)	명칭(미국, 2009)
1	Jurisdictional	Jurisdictional(state to state and federal to state)
2	Computer Evidence Presentation difficulties	Computer evidence presentation difficulties
3	Requirements to 'Fire Up' Original	Requirement for best practices guides and standards
4	Computer Literacy in the Legal Sector	Computer literacy in the legal sector
5	Confidential Records, Business Systems	Confidential records and business systems privacy
6	Telecommunications Act Covering Data	Privacy protection for data transmission laws
7	Criminal Prosecution vs Civil Trial	Criminal prosecution vs. civil litigation
8	Privacy Issues/ Workplace Surveillance	Privacy issues and workplace surveillance
9	Interpretation of Telecommunications Act	Interpretation of laws affecting digital evidence
10	Access and Exchange of Information	Access and exchange of information
11	International Cooperation in Practice	International cooperation in legal practice
12	Revision of Mutual Assistance	Preservation of privacy of clients during digital investigations
13	Contrast of Broadcast vs Communications	Contrast of broadcast vs. communications
14	Do We Need New Offences?	Need to specify new offenses
15	Launching Actions Against Persons Unknown in a Civil Trial	Launching actions against persons unknown in civil litigation
16	Technical Issues	Testing of new tools and techniques
17	Court Reporting Skills and Techniques	Expert witness skills and qualifications

석관과는 달리 분석을 의뢰하는 법조계나 경찰 등의 수사관은 관련 지식을 보유하고 있는 경우가 많지 않으며, 때문에 업무의 비 효율성 및 분석 결과의 이해에 어려움을 겪는 경우가 많다. 또한, 반대로 상호 작용의 어려움 때문에 분석관 역시도 사건의 맥락 등에 대한 이해도가 떨어지는 경우가 다소 존재한다(신지호, 2016). 하지만 이렇듯 디지털 포렌식 업무 내 각 부처간 접점에서 많은 예외사항이 발생하고 있음에도 디지털 포렌식 업무 시, 부처간 이슈 현황이나 중요성 등에 대한 연구는 현재 부재한 상황이다.

III. 연구 방법론

3.1 디지털 포렌식 법률적 이슈의 조작적 정의

디지털 포렌식 분야의 법률적 우선 핵심 이슈사항 도출 및 부서간 우선 이슈사항의 차이를 연구하기 위해 관련 선행연구를 검토하였다. 국내의 경우는 관련 선행연구가 아직 진행되지 않았음을 확인할 수 있었으며, 해외의 경우에는 2003년 호주 내 세 집단(경찰, 정부 관계자, 상업 관계자)의 디지털 포렌식 전문가들이 브레인 스토밍과 회의를

〈표 2〉 디지털 포렌식 분야의 법률적 이슈사항

이슈	이슈 사항	조작적 정의
1	모범 사례 지침과 표준의 필요성	디지털 증거의 증거능력을 확보하기 위한 절차, 프레임워크 등의 모범 사례들과 표준 확립이 필요함
2	법률 종사자들의 디지털 증거 이해 능력	디지털 포렌식 전문가가 증거로 제출한 디지털 증거의 정당성과 증거능력 파악을 위해서는 법률 종사자의 디지털 증거 이해능력이 필요함
3	기업의 기밀에 대한 정보 보호	디지털 증거 수집 시, 기업 기밀이 노출되지 않도록 법 규정의 확립이나 절차의 체계화가 필요함
4	데이터 전송 시 통신 세부정보 보호	데이터의 실시간 전송 중 통신 접속 세부정보들의 보호 규제가 필요함
5	형사소송과 민사소송의 차이점	디지털 증거 소유자에게 사전 고지없이 증거 압수가 가능한 형사소송과 달리, 민사소송은 사전고지 없이 증거 압수가 불가능하기 때문에 디지털 증거에 대한 위·변조 혹은 파기의 가능성이 존재함
6	감시와 프라이버시	디지털 증거 수집 시, CCTV, 개인의 접속기록, 개인정보 등, 무차별적인 수집에 대한 범위의 제한 또는 절차 확립이 필요함
7	디지털 증거에 영향을 미치는 법의 해석	통신 세부정보사항의 정의가 법적으로 명확하지 않기 때문에 해석의 다양성이 존재함
8	정보의 접근과 획득	디지털 증거 확보를 위해 통신회사 및 ISP에 협조 요청 시, 협조 범위 및 수준관련 법률이 필요함
9	법률 부문에서의 국제협력	디지털 증거를 수집을 위해 국가 간 협력 요청 시, 수사 협력을 위한 표준이 필요함
10	디지털 증거 조사 중 개인의 프라이버시 보호	디지털 증거 수색 시 범죄 내용과 무관한 정보노출 범위의 규정 및 법적규제가 필요함
11	디바이스에 따라 적용되는 법의 종류	디지털 포렌식 시, 각 매개체에 따라 적용 법이 다르기 때문에 발생하는 여러 이슈들에 대한 해결 대책 마련이 필요함
12	새로운 위법행위를 구체화할 필요성	기술 발전, 디바이스 다양화 등으로 인해 발생하는 새로운 유형의 사건들에 대해 정확한 파악 후 구체화를 통해 명확한 원인 파악, 증거 추출 및 법제도 정비가 필요함
13	민간 기업의 증거 수집	디지털 포렌식 전문 기업에서, 디지털 범죄 증거를 수집할 때 발생하는 다양한 문제점에 대한 진단 및 해결책이 필요함
14	새로운 포렌식 도구와 기술의 테스트	디바이스 다양화 및 기술의 발전에 대비하기 위해 포렌식 도구 및 기술의 지속적인 검증 및 새로운 포렌식 도구의 개발이 필요함
15	전문가로서의 진출 능력과 자격 요건	디지털 증거 진출과 자격을 위한 전문가선별의 최소한의 기준 확립이 필요함

거쳐 17가지 이슈를 도출한 연구(Brungs and Jamieson, 2005), 그리고 해당연구를 미국 상황에 맞추어 재정의 후, 동일한 그룹 집단에 대해 인터뷰를 실시한 연구(Liles et al., 2009) 등이 존재함을 확인할 수 있었다. 하지만 앞선 선행 연구의 법률적 핵심 이슈사항들은 해외 배경에 맞추어 도출되었다는 점, 기간이 오래되었다는 점, 그리고 해결 된 이슈가 존재할 수도 있는 점에 의거해, 재검토 될 필요가 있었다. 따라서 먼저 국내 배경에 맞추어 국내에 존재하지 않는 관할권과 관련된 위의 <표 1>의 1, 2번 두 이슈 사항을 제외하였으며, 나머지 15개 사항은 국내에서도 최근까지도 논의되고 있는 주제임을 확인한 후(권양섭, 2016a; 김민석, 박석천, 2015; 대검찰청, 2014; 신지호, 2016; 이상미, 2015; 정대용, 2017; 정대회, 어수웅 등, 2016; 조광훈, 2014), 국내 환경에 맞는 예시, 설명과 함께 조작적 정의를 실시하였다(<표 2> 참조). 이 후, 이를 바탕으로 앞선 선행연구와 같이 세 집단 간, 이슈들에 대한 전문가 인터뷰를 실시하였으며, 이를 통하여 각 이슈 별 우선순위와 집단 내에서의 이슈 별 우선순위를 도출하였다.

3.1.1 모범 사례 지침과 표준의 필요성

본 이슈는 디지털 증거의 증거능력을 확보하기 위한 절차, 프레임워크 등의 모범 사례들과 표준 확립의 필요성을 의미한다. 디지털 포렌식 분야에 있어 표준화된 프레임워크, 절차, 프로세스들을 만들려는 노력이 있어 왔다. IOCE(International Organization on Computer Evidence, G8 2000)에서는 법적인 집행자를 대상으로 한 디지털 포렌식 절차모형을 만들었으며, NIJ 2004 Report에서는 분석자를 대상으로 한 디지털 포렌식 절차모형을 언급하고 있다. 국내에서는 검찰청에서 디지털 증거수집 및 분석 규정(대검예규)과 경찰청의 디지털 증거 처리 표준 가이드라인이 존재한다. 검찰청의 규정은 법적절차 관점으로, 경찰청의 규정은 분석가 측면에서의 기술적 부분으로 볼 수 있다. 또한 미 법무부와 경찰 서장 연합에 의해 모범 실무 지침도 발간되었

다. 실제로 이러한 모범 실무를 위한 지침은 여러 출판물과 디지털 포렌식 교육 프로그램을 통해 알려지고 있다. 그러나, 현재 존재하는 표준과 모범 실무 지침이 디지털 포렌식의 모든 부분에 대해 충분히 존재하는지에 대해서 국내에서 논의된 바가 없기 때문에 실증적 확인이 필요한 실정이다.

3.1.2 법률 종사자들의 디지털 증거 이해능력

본 이슈는 디지털 포렌식 전문가가 증거로 제출한 디지털 증거의 정당성과 증거능력 파악을 위해서는 법률 종사자의 디지털 증거 이해능력이 필요하다는 것을 의미한다. 법률 종사자들은 전반적으로 컴퓨터에 대한 충분한 전문 지식을 보유한 경우가 많지 않다. 그러나 디지털 증거의 당위성이나 위력에 대해 파악하기 위해서는 일정수준의 컴퓨터 지식이 요구된다. 또한, 디지털 포렌식 전문가 부족으로 인해 사건 발생시, 수사관들의 실수로 증거의 원본 보존이 안 될 경우도 존재할 수 있다. 그러므로, 디지털 증거와 관련된 사건을 담당하는 관계자는 컴퓨터에 대한 최소한의 이해능력이 필요하다. 본 이슈는 국내에서 여전히 제기되고 있으며 해결을 위해 조직 구조와 업무개선을 위한 연구가 이루어지고 있다(신지호, 2016).

3.1.3 기업의 기밀에 대한 정보 보호

본 이슈는 디지털 증거 수집 시, 기업 기밀이 노출되지 않도록 법 규정의 확립이나 절차의 체계화가 필요하다는 것을 의미한다. 디지털 증거 수집 시, 서버 같은 경우 많은 자료들이 존재하기 때문에 조사 과정에서 기업의 핵심 기술 문서나 개발 중인 사업 자료가 포함될 수 있다. 핵심 기밀이 노출된다면 기업의 생존에 지대한 영향을 미치게 된다. 따라서 기밀자료에 경우, 기업은 보호받길 원하지만 이에 대한 법적 규제가 존재하지 않는다. 그러므로 이에 대해 보호할 수 있는 법 개정이 필요하다.

3.1.4 데이터 전송 시 통신 세부정보 보호

본 이슈는 데이터가 실시간 전송 중일 경우, 해

당 데이터의 보호 법률은 존재하지만 통신 접속 세부정보들은 법률과 같은 보호 규제가 없다는 이슈를 의미한다. 데이터를 전송하는 과정에서 실시간 정보를 획득하는 것을 감청이라고 한다. 이에 대해 국내에서는 통신비밀보호법에 의거한 감청 영장이 존재하며 미국에서도 감청법(Wiretap Act)에서 이에 대한 내용을 포함하고 있다. 통신에서는 크게 전송 중인 데이터와 이미 전송이 완료된 데이터에 대해 다른 분류를 가지며, 전송 데이터와 통신접속정보로 나뉜다. 미국에서는 양쪽 모두에 관하여 실시간, 전송 완료된 데이터로 나누어 규정하고 있지만 국내에서는 실시간 획득 가능한 통신접속정보에 대해서는 언급되지 않고 있다. 하지만 이러한 통신접속정보로부터 개인의 프라이버시가 노출이 될 수 있기 때문에 이에 대한 법 개정이 필요하다.

3.1.5 형사소송과 민사소송의 차이점

형사소송은 디지털 증거 소유자에게 사전 고지 없이 해당 증거 압수가 가능하지만, 민사소송은 그러지 않다. 따라서 본 이슈는 디지털 증거에 대한 위·변조 혹은 파기의 가능성이 존재한다는 것을 의미한다. 이는 형사소송 사건에서의 디지털 증거 개시와 민사소송사건에서의 디지털 증거 개시에 차이점이 존재하기 때문인데, 형사사건에서는 디지털 증거를 소유하고 있는 사람에게 사전고지 없이 해당 증거를 압수할 수 있는 데 비해 민사사건에서는 디지털 증거를 소유하고 있는 사람이 원고가 찾고자 하는 전자적 증거가 어떤 것인지 미리 알고 증거 소유자가 자신의 불법 행위와 관련된 증거를 변경 또는 파기할 수 있기 때문이다. 예를 들어, 통합 진보당의 당 내 부정사건 시 1차 영장, 2차 영장을 통해 최종적으로 기록매체를 압수하였는데 이때, 그 때까지 상당량의 증거 인멸에 대한 가능성을 배제할 수 없었던 것을 들 수 있다(대검찰청, 2014). 또한, 조사자의 권력이라는 차이점이 존재한다. 형사소송은 수색 영장, 감청영장 등 다양한 힘을 쓸 수 있지

만 민사소송은 데이터를 합법적으로 얻기 위한 방법이 다양 하지 않다. 이러한 형사소송과 민사소송의 차이점에서 나타나는 여러 어려운 점들을 해결해야 할 필요성이 존재한다.

3.1.6 감시와 프라이버시

본 이슈는 디지털 증거를 수집하기 위해 CCTV, 개인의 접속기록, 개인정보 등, 무차별적인 수집에 대한 범위 제한 또는 절차적 충분성에 대한 이슈를 의미한다. 디지털 포렌식 분야에서 개인정보 수집 및 검색이 허용되는 범위에 대한 언급은 개인정보보호법에 명시 되어있다. 개인정보라 함은 개인정보보호법에 “살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상을 통하여 개인을 알아볼 수 있는 정보”라고 정의가 되어 있다. 여기서 중요한 것은 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다는 내용이다. 또한 개인정보보호법은 특별법이 아닌 일반법이 기 때문에 전 국민에 통용되지만 애매함이 존재하며 개인정보보호법이 적절하게 제정 시행되었는지에 대한 테스트가 부족하다. 또한, 기업의 입장에서 사건 사고는 내부자의 소행으로 매우 많이 일어나고 내부 보안에 취약하기 때문에(윤한성, 2007) 이에 대한 감시를 어느 정도 선까지 수행해야 하는가에 대한 이슈도 포함되어 있다. 국내에서 역시 최근까지 이러한 증거의 무차별적 수집 관련 문제가 발생하고 있으며 해당 문제가 관련 법률 미비에 기인한다고 판단하고 있으며 꾸준한 논의가 이루어지고 있는 실정이다(정대회, 이상미, 2015).

3.1.7 디지털 증거에 영향을 미치는 법의 해석

본 이슈는 통신 세부정보 사항에 있어 ‘통신의 시작과 끝의 정의’, ‘이메일의 열람 유무 정의’ 등 법적으로 명확화 한 것이 없기 때문에 이에 따라 해석의 다양성이 존재하는 것에 대한 이슈를 의미한다. 통신 세부정보 사항에 있어서 세부적 구

분의 불확실한 정의로 인해 법적으로 명확화 한 것이 없다. 이에 따라 해석의 다양성이 존재하므로 판결에 상당한 영향을 미칠 수 있는 가능성이 존재한다. 그러므로 이에 대한 법적 기준 마련이 필요하다.

3.1.8 정보의 접근과 획득

본 이슈는 디지털 증거를 확보하기 위해 통신회사나 ISP에 협조 요청할 시, 정보의 범위와 그 수준과 관련된 법률이 존재하지 않아 디지털 증거에 대한 접근과 확보가 어려운 것에 대한 이슈를 의미한다. 디지털 증거 수집 시 통신회사나 ISP의 협조가 필요한 경우가 존재한다. 그러나 협조 시 고객들의 개인정보에 대한 보호 측면에서 통신비밀보호법과 개인정보보호법이 역시도 언급되고 있다. 미국에서는 전자통신프라이버시법(Electronic Communication Privacy Act of 1986)을 통해 데이터 통신 보호 및 ISP의 협조에 대해 언급하고 있다. 그러나 법이 명확하지 않음에 의해 국내에서 여러 문제가 발생하고 있는데, 이러한 문제의 대표적 예가 바로 카카오톡 감청 사건이다. 통신비밀보호법에 따라 시행된 감청영장으로 전기통신 사업법에 해당하는 통신회사나 ISP는 개인정보를 제공해야 한다. 그러나 이로 인하여 개인의 프라이버시 침해를 염두에 둔 개인 이용자들은 카카오톡 사용을 지양 하는 등 다양한 우려의 목소리를 내고 있다. 최근 들어 수사에 필요한 내용만 전달하고 나머지는 암호화하여 볼 수 없도록 상호 합의했지만, 해당 이슈와 같은 사항은 상호 합의가 아닌 법적인 언급이 필요할 것으로 보여진다.

3.1.9 법률 부문에서의 국제협력

본 이슈는 디지털 증거의 특성 상, 증거를 수집을 위해 국가 간 협력이 필요할 때가 존재하지만 각 국가의 제정법이 다르므로 수사 시 협력할 수 있는 표준이 필요하다는 이슈를 의미한다. 디지털 증거는 특성 상 국가 경계를 쉽게 통과하

로 증거 수집을 위해서 국가 간 협력이 필요할 경우가 존재한다. 그러나 국가별 법이 상이하기 때문에 증거 수집 시 협조에 난항을 겪을 수 있다. 때문에 국제적 표준이나 법률이 필요하다. 현재 공권력 측면에서 인터폴이 해당 부분에 대해 국제협력을 담당하고 있으나 민사관계에서는 국제협력 대안이 현재 존재하지 않는다. 따라서 세계적으로 국제 협력수사의 중요성이 강조되고 제도화 되고 있지만, 국내는 아직 관련 법적 근거가 미비하여 이러한 절차가 국내 법제 하에서 허용되는지, 증거능력의 입증은 어떻게 이루어져야 하는지 다양한 문제가 제기되고 있다(정대용, 2017).

3.1.10 디지털 증거 조사 중 개인의 프라이버시 보호

본 이슈는 디지털 증거 수색 과정 시 범죄 내용과 관련 없는 부분의 노출에 대해 범위의 규정이나 법적규제가 존재하지 않음에 대해 생기는 이슈를 의미한다. 디지털 매체로부터 디지털 증거를 수색하는 과정 중 개인의 프라이버시가 노출되고 있다. 국내에서 여성의 노출 부위를 촬영하는 것으로 의심된 한 남성이 경찰에 붙잡혀 개인 휴대폰을 샅샅이 수색 당하는 과정에서 개인과 관련된 프라이버시가 보호받지 못한 채로 전부 노출되었다. 정작 여성의 노출 부위를 촬영한 사진은 없었고 고스란히 개인의 정보만 노출된 셈이다. 이러한 사건들의 빈도가 높아지고 있으므로 이러한 측면에 대한 대책을 마련해야 한다. 국내 역시 수사기관들이 범죄와 관련 없는 개인정보까지 손쉽게 획득할 수 있다는 점이 문제점으로 지적되어 오고 있다(조광훈, 2014).

3.1.11 디바이스에 따라 적용되는 법의 종류

본 이슈는 디지털 포렌식은 컴퓨터, 스마트폰, TV, IPTV 등 다양한 디바이스에 대해 이루어지는데 각 매개체에 따라 적용되는 법이 다르므로 이에 대해 발생하는 여러 이슈들에 대한 해결 대

책 마련을 의미한다. 예를 들어, 국내에서 텔레비전은 방송법에 해당하고, 인터넷(IP)TV는 인터넷 멀티미디어 방송사업법에 해당하고, 휴대폰은 전기통신사업법에 해당하고, 컴퓨터는 정보통신망법에 해당한다. 이처럼 방송과 통신의 각 서비스별로 법을 달리 하다 보니 각 디바이스에 발생한 상황에 따라 어떠한 법을 적용해야 하는지 복잡해질 수밖에 없다. 그리고 인터넷 동영상 서비스 같은 경우에는 어떠한 법을 적용해야 하는지 수많은 논란이 발생할 수밖에 없다. 이러한 문제의 원인은 현재의 법이 사업자 중심이기 때문이다. 그러므로 이를 이용자 중심으로 패러다임을 변경해야 할 필요성이 존재한다.

3.1.12 새로운 위법행위를 구체화할 필요성

본 이슈는 기술의 발전, 디바이스의 다양화로 인해 발생할 새로운 유형의 사건들에 대해 정확히 파악 후 구체화하지 않는다면 명확한 원인 파악과 증거 추출이나, 관련법의 미미로 처벌이 힘들어지는 것에 대한 이슈를 의미한다. 기술의 발달에 따라 범죄 역시도 다양해지고 있다. 이에 따라 새로 발생한 위법행위에 대해 구체적으로 파악하기 위하여 노력하고 대안을 마련하지 않는다면 수많은 범죄에 대한 정당한 판결이 어려울 것이다. 따라서 새로운 위법 행위를 명확히 파악 후 관련 법적 대응을 마련해야 한다. 국내 역시도 유비쿼터스나 IoT와 같은 새로운 환경화에서의 디지털 포렌식 기술 및 법제를 꾸준히 연구 및 논의 해 오고 있는 실정이다(권양섭, 2016b; 김민석, 박석천, 2015).

3.1.13 민간 기업의 증거 수집

본 이슈는 디지털 포렌식 전문 기업에서, 디지털 범죄 증거를 수집할 때 발생하는 다양한 문제점에 대한 해결책이 필요하다는 이슈를 의미한다. 비정부 조직에서 발생하는 대부분의 사건은 민사소송으로 진행된다. 그러나, 민사소송사건에서의 디지털 증거에 관한 증거 수집은 여러 가지 애로

사항을 보유하고 있다. 원고의 입장에서는 사건과 관련된 디지털 증거가 어떤 증거인지, 이 증거가 어디에 존재하는지, 이 증거를 누가 관리하고 있는지 등을 예시로 들 수 있다. 또한, 민사사건에서는 형사사건보다 디지털 증거가 분실되거나 파괴될 가능성도 높다. 또한, 민사소송을 하기 위해서는 신분을 알아야 하고, 모를 경우에는 수행되지 않는다. 이것은 비정부 조직의 증거 수집 시 주요 장애물이고 해결책이 개발되어야 할 부분이다.

3.1.14 새로운 포렌식 도구와 기술의 테스트

본 이슈는 디바이스 다양화 및 기술의 발전이 다양한 범죄를 야기함에 따라 기존의 포렌식 도구와 기술 역시도 발전하기 위해 새로운 도구 개발을 지속하고 검증해야 한다는 것을 의미한다. 법적으로 타당한 포렌식 도구가 되기 위해서는 반드시 정의되어야 하고 예측 가능해야 하며 반복되고 재검증 가능해야 한다. 이러한 측면에 대해서 미국에서는 미국표준기술연구소(NIST: National Institute of Standards and Technology)에서 운용 중인 컴퓨터 포렌식 도구 검증 프로그램(CFTT: Computer Forensics Tool Testing program)을 통해 검증 방법을 개발하고 있다. 그러나 새로운 범죄가 계속 발생하고 있고, 그 수단과 방법이 다양해지는 만큼 새로운 포렌식 도구의 개발과 테스트가 지속되어야 한다. 예를 들어, 스마트폰, 태블릿 PC와 같은 스마트 기기의 경우, 오픈소스 소프트웨어를 사용한다고 할지라도 제조사 마다 그 특성이 조금씩 다르다. 따라서 안드로이드 기기에서 디지털 증거를 획득하고 분석하는 방법은 그 제조사별, 모델별로 다양성과 복잡성이 존재한다. 따라서 이와 같은 문제점들로 인한 효율적인 디지털 증거 수집 방안 및 도구의 타당성 문제는 현재 세계적인 이슈라고 할 수 있다(어수용 등, 2016).

3.1.15 전문가로서의 진술 능력과 자격 요건

본 이슈는 디지털 증거 진술과 자격을 위한 전문가선별의 최소한의 기준 확립이 필요하다는 것

을 의미한다. 변호사 수임한 사건에서 전문가에 대해 어떤 규정이 적용되는지에 상관없이 모든 전문가들은 먼저 전문가로서의 자격을 갖춰야만 향후 법정에서 전문가 증언을 할 수 있는 것과 같이 디지털 증거 증언가로서의 전문가 고용은 매우 중요한 부분이다. 디지털 포렌식 전문적인 기술 교육 이수, 디지털 증거 분석에 대한 경력, 그리고 해당 분야에 대한 전문성도 증명할 수 있는 전문가여야 한다. 또한 법정에서 진행되는 전문가 증언은 전문가의 지식뿐 아니라 논리적 성향 및 표현력도 중요하기 때문에 전문가로서의 진술 능력 또한 중요하다고 할 수 있다.

3.2 자료의 수집 및 전문가 그룹

3.2.1 조사 대상

본 연구의 인터뷰 대상은 디지털 포렌식 관련 종사자로 정하였다. 전문가로 범위를 좁혀 실시하는 것이 조금 더 정확한 연구에 적합하나 국내에 디지털 포렌식이 도입된 지 오래되지 않은 점 때문에 전문가로 칭할 수 있는 조사 대상자가 소수이므로 종사자로 그 범위를 확대하였다. 디지털 포렌식 종사자란 디지털 포렌식 관련 업무를 수행 중이거나 해당 분야에 대한 교육을 받은 경찰, 정부 관계자, 상업 관계자가 그 대상이다. 또한, 대검 예규인 디지털 증거 수집 및 분석 규정 제1장 제6조에서 언급하고 있는 디지털 포렌식 수사관의 조건에 해당하는 사람-“검찰청 디지털수사과에서 실시하는 ‘디지털 포렌식 전문가 양성 과정’과 국내·외 컴퓨터 관련 교육과정을 이수한 자로서 디지털포식 관련지식이 충분하다고 인정되는 자”, “3개월 이상의 디지털 포렌식 수사실무를 수행한 경력이 있는 자”-도 본 인터뷰 대상에 포함된다.

3.2.2 수집 방법

디지털 포렌식 분야의 법률적 이슈사항의 집단 별 중요도 차이 측정을 위하여 4집단(경찰, 민

간기업, 정부 및 공공기관, 법조계)의 디지털 포렌식 종사자 대상 인터뷰를 2015년 11월 10일부터 11월 28일까지 19일간 실시하였다. 인터뷰는 포렌식 분야의 전문가들과 인터뷰할 내용을 질의화 하여 인터넷을 이용하여 배포 및 회수하였다. 수집된 건수는 총 29건이었으며, 세부 그룹별 분류는 경찰 15명, 민간기업 9명, 정부 및 공공기관 3명, 법조계 2명이었다. 분석 툴은 SPSS 21과 Microsoft Office Excel 2013을 사용하였고, 각 이슈의 중요도는 5-point Likert Scale로 측정하였다. <표 3>는 인터뷰 대상자의 인구통계학적 분석을 나타낸다.

<표 3> 인구통계학적 데이터 분석

성별 (단위: 명)	남	23
	여	6
연령	20대	6
	30대	15
	40대	8
	50대	0
직업	경찰	15
	정부 공공기관	3
	민간기업	9
	법조계	2
학력	대학 졸업	19
	대학원 재학 중	2
	대학원 졸업	8
디지털 포렌식 업무 경력	2년 미만	9
	2년 이상 4년 미만	9
	4년 이상 6년 미만	9
	6년 이상 8년 미만	0
	8년 이상	2

IV. 연구 결과

4.1 조사 결과

우선 본 인터뷰 29명의 조사 결과에 대한 내용

중, 정량적으로 참고할 수 있는 질의형 데이터를 통해 본 조사의 정규성을 확인하였다. 본 연구는 데이터가 많거나 적다고 보기 애매한 측면(N = 29, 10 < N < 30)이 있었기 때문에 두 가지 방법을 통해 정규성을 확인하였다. Kolmogorov-Smirnov test 결과와 Shapiro-Wilk test 결과 모두 유의한 것으로 나타나 비모수 검정을 실시하였다(<표 4> 참조).

<표 4> 정규성 확인 데이터 값

이슈	Kolmogorov-Smirnov test			Shapiro-Wilk test		
	통계량	DF	유의확률	통계량	DF	유의확률
1	.419	29	.000	.638	29	.000
2	.399	29	.000	.663	29	.000
3	.300	29	.000	.768	29	.000
4	.212	29	.002	.875	29	.003
5	.208	29	.002	.853	29	.001
6	.208	29	.003	.871	29	.002
7	.291	29	.000	.794	29	.000
8	.379	29	.000	.692	29	.000
9	.348	29	.000	.725	29	.000
10	.209	29	.002	.870	29	.002
11	.224	29	.001	.833	29	.000
12	.279	29	.000	.810	29	.000
13	.196	29	.006	.861	29	.001
14	.359	29	.000	.715	29	.000
15	.360	29	.000	.715	29	.000

4.2 결과 분석

4.2.1 국내의 우선순위 결과

분석 결과를 통해 우선순위를 도출하기 위해 대응 K 표본에 대한 비모수적 순위 분석방법인 Kendall's W test를 실시하였다. 여기서는 차후 호주의 Brungs-Jamieson(2005) 연구와 미국의 Liles(2009) 연구와의 비교를 위해 중요도를 1점(매우 중요함)에서 5점(매우 중요하지 않음)으로 데이

터를 변형하였다. 해당 방법으로 도출된 값은 아래 <표 5>와 같다.

<표 5> 각 이슈에 대한 우선순위 도출

	이슈 명	평균 순위
1	모범 사례 지침과 표준의 필요성	5.91(1)
2	법률 종사자들의 디지털 증거 이해능력	6.66(3)
3	기업의 기밀에 대한 정보 보호	7.47(7)
4	데이터 전송 시 통신 세부정보 보호	10.16(14)
5	형사소송과 민사소송의 차이점	8.83(11)
6	감시 대 프라이버시	10.19(15)
7	디지털 증거에 영향을 미치는 법의 해석	7.98(8)
8	정보의 접근과 획득	6.21(2)
9	법률 부문에서의 국제협력	6.83(6)
10	디지털 증거 조사 중 개인의 프라이버시 보호	9.52(12)
11	디바이스에 따른 적용되는 법의 종류	8.48(9)
12	새로운 위법행위를 구체화할 필요성	8.64(10)
13	민간 기업의 증거 수집	9.57(13)
14	새로운 포렌식 도구와 기술의 테스트	6.81(5)
15	전문가로서의 진술 능력과 자격 요건	6.76(4)

각 법률적 이슈사항 중 우선순위가 가장 높게 나온 것은 ‘모범 지침 사례와 표준의 필요성’이다. 그 다음으로 ‘정보의 접근과 획득’, ‘법률 종사자들의 디지털 증거 이해능력’이 중요한 것으로 나타났다. 우선순위가 가장 낮게 나온 이슈는 ‘데이터 전송 시 통신 세부정보 보호’인 것으로 나타났다. 그 다음으로 낮게 나온 이슈는 ‘감시 대 프라이버시’와 ‘민간 기업의 증거 수집’인 것으로 나타났다.

이를 그룹 별로 분류하여 이슈 간 우선순위를 분석 해보았다. 아래 <표 6>은 그룹 별로 각 이슈에 대한 우선순위를 나타낸다. 표 안의 값은 Kendall's W test를 통해 나타난 값이고, 괄호 안의 값은 순위를 나타낸다.

〈표 6〉 그룹별 우선순위 비교

이슈	경찰	정부 공기업	민간기업	법조계
1	5.27(1)	7.67(8)	6.56(2)	5.25(3)
2	5.57(2)	9.67(11)	7.11(5)	8.25(6)
3	7.63(8)	7.33(6)	7.06(4)	8.25(6)
4	10.47(15)	9.33(10)	9.56(14)	11.75(13)
5	8.77(9)	7.33(6)	9.44(13)	8.75(9)
6	10.00(13)	13.33(15)	8.78(11)	13.25(15)
7	6.87(4)	10.83(13)	8.33(9)	10.50(12)
8	5.97(3)	5.33(2)	7.11(5)	5.25(3)
9	7.33(7)	3.83(1)	7.83(8)	3.00(1)
10	10.40(14)	10.50(14)	7.22(7)	11.75(13)
11	8.80(10)	5.33(2)	8.94(12)	8.75(9)
12	9.27(11)	6.00(4)	8.44(10)	8.75(9)
13	9.40(12)	9.67(12)	10.11(15)	8.25(6)
14	7.03(5)	7.67(8)	6.50(1)	5.25(3)
15	7.23(6)	6.17(5)	7.00(3)	3.00(1)

위의 <표 6>에 의하면 경찰 그룹은 우선순위가 가장 높은 이슈로 ‘모범 사례 지침과 표준의 필요성’을 뽑았고, 우선순위가 낮은 이슈는 ‘데이터 전송 시 통신 세부정보 보호’로 나타났다. 정부 및 공기업에서 우선순위가 높은 이슈는 ‘법률 부문에서의 국제 협력’인 것으로 나타났고, 우선순위가 낮은 이슈는 ‘감시 대 프라이버시’로 나타났다. 민간 기업은 우선순위가 높은 이슈로 ‘새로운 포렌식 도구와 기술의 테스트’로 나타났고, 우선순위가 낮은 이슈로 ‘민간 기업의 증거 수집’으로 나타났다. 마지막으로 법조계에서는 ‘법률 부문에서의 국제 협력’, ‘전문가로서의 진술 능력과 자격 요건’이 우선순위가 높은 이슈로 뽑혔고, ‘감시 대 프라이버시’ 이슈가 가장 우선순위가 낮은 이슈로 나타났다. ‘모범 사례 지침과 표준의 필요성’ 이슈에 대해 경찰과 민간기업, 법조계는 각 1순위, 2순위, 3순위로 상위권 위치하였으나 정부 공기업 그룹은 8순위로 순위가 낮았다. 반대로 ‘법률 부문에서의 국제 협력’ 이슈에 대해 1순위로 뽑았다. 반면에 경찰과 민간기업은 각각 해당 이슈에 대해 7순위, 8순위로 나타났다. ‘정보의 접근과 획득’ 이슈에 대해서는 각각 3순위, 2순위, 5순위, 3순위로 모든

그룹에서 상위권으로 나타났다. ‘디지털 증거 조사 중 개인의 프라이버시 보호’ 이슈에 대해서는 경찰과 정부 공기업, 법조계 그룹이 각각 14순위, 12순위로 나타난 데 비해 민간기업그룹에서는 7순위로 비교적 우선순위가 높았다. ‘새로운 위법행위를 구체화할 필요성’ 이슈에 대해서는 정부 공기업 그룹이 4순위로 나타난 데 비해 경찰과 민간기업, 법조계 그룹에서는 각각 11순위, 10순위, 9순위로 나타났다. ‘디바이스에 따라 적용되는 법의 종류’ 이슈에 대해서는 정부 공기업 그룹이 2순위로 나타났지만 경찰과 민간기업, 법조계 그룹에서는 각 10순위, 12순위, 9순위로 나타났다. ‘민간 기업의 증거 수집’ 이슈에 대해서는 법조계를 제외한 그룹이 12순위, 12순위, 15순위로 하위권으로 나타났다. 법조계만 6순위로 나타났다. 각 이슈에 대해 각 그룹별로 어떠한 차이가 있는지를 알아보기 위하여 독립된 세 개 그룹 이상의 크기를 비교하는 비모수적 검정 방법인 Kruskal-Wallis test 방법을 이용하였다. 아래 <표 7>은 Kruskal-Wallis test로 인해 도출된 값을 나타낸다. 이를 통해 각 그룹별 해당 이슈의 중요도 평균값을 알 수 있다. 해당 값이 높을수록 해당 그룹이 각 이슈에 대해 중요하게 생각하고 있음을 의미한다.

〈표 7〉 그룹별 각 이슈에 대한 중요도 값

이슈	경찰	정부 공기업	민간기업	법조계
1	16.80	9.00	14.50	12.75
2	17.17	8.33	14.44	11.25
3	14.60	12.00	17.17	12.75
4	14.00	14.50	17.33	12.75
5	15.37	14.50	14.67	14.50
6	14.73	9.00	18.33	11.00
7	16.90	7.00	16.22	7.25
8	16.30	11.83	14.11	14.00
9	14.07	16.83	14.61	21.00
10	13.30	9.50	20.17	12.75
11	14.40	17.00	15.67	13.50
12	14.37	16.83	15.89	13.00
13	16.00	13.00	13.78	16.00
14	14.80	10.67	16.83	14.75
15	13.67	14.67	16.00	21.00

4.2.2 호주, 미국, 한국의 우선순위 결과 비교
 <표 8>은 해당 연구의 결과와 호주의 Brungs-Jamieson(2005)의 연구 결과, 그리고 미국의 Liles(2009)의 연구를 3개의 그룹(경찰, 정부, 민간)에서 Kendall's W test를 통한 결과비교를 제시한 것이다. 각 값은 평균 순위를 의미하며 괄호 값은 해당 이슈의 중요도 순위를 의미한다. 해당 분석은 점수가 낮을수록 중요하다는 것을 의미하며, 기존 Liles(2009) 연구에서 응답이상으로 제외되었던 'Launching actions against persons unknown in civil litigation' 이슈와 관할권 관련 이슈로써 국내 현황과 연관 없는 'Jurisdictional', 그리고 'Presentation Difficulties' 이슈는 제외하였다.

해당 결과는 세 연구의 kendall's W test 결과값으로 알 수 있는 차이점을 보여준다. 이슈 2번 '법률 종사자들의 디지털 증거 이해능력'에 대해서는 경찰 그룹에서 미국과 호주는 각각 7순위, 9순위로 중간 우선순위에 머물렀으나 한국에서는 2순위로 도출되었다. 이슈 4번 '데이터 전송 시 통신 세부 정보보호'에 대해서는 경찰 그룹에서 한국과 호주에서는 각각 15순위, 10순위로 나타났으나 미국에서는 2순위로 나타났다. 또한, 민간기

업 그룹에서는 해당 이슈에 대해 미국과 호주가 각각 5순위, 3순위로 나타났으나 한국에서는 14순위로 나타났다. 이슈 6번 '감시 대 프라이버시'에 대해서는 민간기업 그룹에서 한국과 미국에서는 각각 11순위, 13순위로 나타났으나 호주에서는 1순위로 나타났다. 이슈 7번 '디지털 증거에 영향을 미치는 법의 해석'에 대해서는 경찰 그룹에서 한국, 미국, 호주가 각각 4순위, 3순위, 1순위로 상위권으로 나타났다. 그러나 정부 공기업 그룹에서는 미국과 호주가 해당 이슈에 대해 각각 1순위, 2순위로 둔 반면에 한국에서는 13순위로 나타났다. 이슈 9번 '법률 부문에서의 국제협력'에 대해서는 정부 공기업 그룹에서 한국과 호주에서 1순위로 나타났으나, 미국에서는 9순위로 나타났다. 이슈 11번 '디바이스에 따른 적용되는 법의 종류'에 대해서는 정부 공기업 그룹에서 미국과 호주에서 각각 16순위, 12순위로 나타났으나 한국에서는 2순위로 나타났다. 이슈 15번 '전문가로서의 진출 능력과 자격 요건'에 대해서는 경찰 그룹에서 미국과 호주에서는 각각 13순위, 16순위로 나타났으나 한국에서는 6순위로 나타났다.

<표 8> 국가 간 그룹별 우선순위 비교

이슈 번호	경찰			정부 공기업			민간기업		
	한국 (Lee)	미국 (Liles)	호주 (B-J)	한국 (Lee)	미국 (Liles)	호주 (B-J)	한국 (Lee)	미국 (Liles)	호주 (B-J)
1	5.27(1)	5.08(1)	11.00(15)	7.67(8)	9.33(11)	11.50(13)	6.56(2)	7.42(7)	12.67(15)
2	5.57(2)	7.42(7)	9.33(9)	9.67(11)	8.94(10)	12.25(14)	7.11(5)	7.03(4)	10.00(11)
3	7.63(8)	7.08(5)	10.33(12)	7.33(6)	6.67(4)	8.00(8)	7.06(4)	5.68(2)	13.00(17)
4	10.47(15)	5.23(2)	10.00(10)	9.33(10)	7.56(7)	6.50(6)	9.56(14)	7.08(5)	6.00(3)
5	8.77(9)	11.50(15)	10.67(14)	7.33(6)	11.78(15)	13.00(16)	9.44(13)	10.34(12)	7.00(5)
6	10.00(13)	9.23(10)	7.33(7)	13.33(15)	7.50(6)	10.25(11)	8.78(11)	10.53(13)	4.00(1)
7	6.87(4)	6.73(3)	4.33(1)	10.83(13)	4.89(1)	4.25(2)	8.33(9)	7.34(6)	5.00(2)
8	5.97(3)	9.27(11)	6.00(4)	5.33(2)	10.94(13)	6.75(7)	7.11(5)	5.26(1)	12.33(14)
9	7.33(7)	6.85(4)	5.33(2)	3.83(1)	7.72(9)	3.25(1)	7.83(8)	10.55(14)	9.67(10)
10	10.40(14)	9.96(12)	10.00(10)	10.50(14)	10.06(12)	6.00(5)	7.22(7)	7.92(8)	8.67(7)
11	8.80(10)	12.50(16)	7.00(5)	5.33(2)	12.33(16)	10.50(12)	8.94(12)	12.92(16)	10.67(13)
12	9.27(11)	11.46(14)	10.33(12)	6.00(4)	11.33(14)	8.50(9)	8.44(10)	11.11(15)	12.67(15)
14	7.03(5)	7.35(6)	8.67(8)	7.67(8)	6.00(2)	10.00(10)	6.50(1)	6.26(3)	6.67(4)
15	7.23(6)	9.96(13)	3.33(16)	6.17(5)	7.61(8)	12.75(15)	7.00(3)	8.00(9)	7.00(5)

V. 토의 및 시사점

5.1 연구 결론

5.1.1 국내의 우선순위 결과 비교

국내 디지털 포렌식 분야의 우선순위 결과와 비교 해 보았을 때, 국내 디지털 포렌식 분야의 법률적 이슈사항 중 가장 중요도가 높게 나온 이슈사항은 ‘모범 사례 지침과 표준의 필요성’으로 나타났다. 인터뷰를 통해 이는 현재 디지털 포렌식은 다양한 분야의 사건에 적용되고 있으나 이 다양성에 적용되는 프레임워크나 모범 사례 지침이 없기 때문임을 알 수 있었다. 따라서 현재 몇 가지 대법원 판례를 기반으로 해석에 의존하고 있는 실정인데, 현재 추세는 디지털 포렌식의 관련 법률 및 판례가 계속 강화되는 방향으로 변화하고 있고, 기술의 발달 및 새로운 매체의 등장으로 새로운 법률과 절차적 환경 또한 계속 변화하고 있기 때문에, 디지털 포렌식은 디지털 증거의 분석 절차가 해당 증거에 대한 정확성과 신뢰에 근거를 제공하는 만큼 이러한 모범 사례 지침과 표준이 필요하다는 것을 유추할 수 있었다. 반대로 가장 중요도가 낮게 나온 이슈 사항은 ‘데이터 전송 시 통신 세부정보보호’로, 이는 통신 상 데이터가 개인의 프라이버시와 관련된 정보기 때문에 보호하고 있지만 세부정보의 보호와 동시에 성능까지 보장하는 표준이나 기법이 나오지 않은 상황에서 법률적으로 규정할 수 없기 때문임을 알 수 있었다. 따라서 굳이 세부정보를 보호하려 하기보다는 법률적 증거 능력이 필요할 시 해당 데이터에 대한 세부정보를 얻을 수 있는 법률적 절차만 형성하면 될 것임을 유추할 수 있었다.

국내 디지털 포렌식 분야에 종사자들을 네 그룹으로 나누어 그 우선순위를 비교 해 보았을 때, ‘모범 사례 지침과 표준의 필요성’에 대해서 정부 및 공기업 그룹이 타 그룹(1순위, 2순위, 3순위)에 비해 낮은 순위(8순위)로 나타났다. 대신 정부 및 공기업 그룹에서는 1순위로 ‘법률 부문

에서의 국제 협력’을 뽑았다. 모범 사례 지침과 표준을 주로 만드는 그룹임에도 불구하고 이러한 낮은 순위가 나타난 것은 국제 협력이 우선시 되어야 국제적으로 효력을 발휘할 수 있는 모범 사례 지침과 표준을 만들 수 있기 때문임을 유추할 수 있었다. ‘정보의 접근과 획득’ 이슈에 대해서는 모든 그룹에 대해서 상위권으로 나타났다. 이는 네트워크 내 디지털 증거가 존재하는 경우가 많기 때문에 증거를 확보하기 위해서는 필수적으로 통신회사나 ISP의 협조가 필요하기 때문임을 판단할 수 있었다. 그러나 우선순위가 점점 높아지는 상황으로 보아 아직까지도 해당 이슈에 대한 해결방안이 없는 것으로 파악된다. ‘새로운 포렌식 도구와 기술의 테스트’ 이슈에 대해서는 민간기업 그룹에서 1순위, 법조계에서는 3순위, 경찰과 정부 공기업 그룹에서는 각각 5순위, 8순위로 나타났다. 이는 각 그룹의 주요 업무가 다르기 때문으로 판단할 수 있었다. 민간기업 그룹은 디지털 포렌식을 통해 기업의 운영을 이어가기 때문에 해당 기술의 검증이 매우 중요한 반면 경찰, 정부 공기업 그룹에서는 해당 기술이 민간 기업처럼 운영에 필수적인 요소는 아니기 때문임을 유추할 수 있었다. 또한, 국내에서의 경찰과 법조계의 관점의 차이도 살펴 볼 수 있었다. 국내는 검찰과 경찰의 이해관계가 주요 이슈이기 때문에 분석해 볼 필요가 있다. 대다수 이슈에 대해서는 우선순위가 유사했다. 그러나 몇몇 차이가 나는 이슈를 살펴보면, 경찰은 가장 우선순위가 높은 이슈로 ‘모범 사례 지침과 표준의 필요성’을 뽑았지만, 법조계에서는 ‘법률 부문에서의 국제협력’을 가장 높은 우선순위로 뽑았다. 해당 이슈에 대해서 경찰은 7순위로 낮게 두었다. 또한, ‘전문가로서의 진출 능력과 자격요건’ 이슈에 대해서 경찰은 6순위로 두었으나, 법조계에서는 1순위로 두었다. 그리고, ‘민간 기업의 증거 수집’ 이슈에 대해 경찰은 12순위로 두었으나, 법조계에서는 6순위로 두었다. 해당 차이는 직업의 관점 상 일반 적이나, 우선순위가 높게 나온

핵심 이슈들이다. 따라서, 해당부분의 관점 차를 좁히기 위한 노력이 수반되어야 할 것임을 판단할 수 있었다.

5.1.2 한국, 미국, 호주의 우선순위 결과 비교

디지털 포렌식 분야에서의 우선순위에 대한 국가별 비교 결과를 살펴보면 경찰 그룹에서 ‘모범 사례 지침과 표준의 필요성’에 대해 한국과 미국에서는 1순위로 뽑았지만 호주에서는 15순위로 나타났다. 이는 디지털 포렌식이 태동하던 초창기 시기에는 모범 사례 지침과 표준보다는 디지털 증거와 연관이 되어 있는 법에 대해서 어떻게 해석해야 하는지가 가장 시급했기 때문으로 판단해 볼 수 있다. 이에 대한 증거로 위와 관련된 있는 이슈 7번 ‘정보의 접근과 획득’에 대해서는 미국의 경찰, 정부 공기업, 민간기업 그룹 모두가 1순위 혹은 2순위로 나타난 것을 볼 수 있다. 다만 이 이슈에 대해서는 시간이 흐를수록 점점 우선순위가 감소하고 있는데 이는 점차 디지털 포렌식 분야가 확보되면서 단순히 디지털 증거를 확보하는 것에 급급했던 시기에서 벗어나 다양한 분야의 발생과 여러 이슈의 발생으로 인한 것으로 파악해 볼 수 있다. ‘법률 부문에서의 국제 협력’이슈에 대해서는 정부 공기업 그룹에서 한국과 호주가 1순위로 나타난 데 비해 미국에서는 9순위로 나타났다. 대신 미국의 정부 공기업 그룹에서는 1순위로 ‘정보의 접근과 획득’ 이슈로 나타났는데 연구당시 미국의 상황이 디지털 증거의 확보에 조금 더 초점이 맞춰져 있었기 때문인 것으로 판단할 수 있다. 이를 뒷받침하기 위해 이슈 14번 ‘새로운 포렌식 도구와 기술의 테스트’가 2순위인 것을 언급할 수 있다. 이슈 7번과 14번은 모두 디지털 증거를 확보하는 데 직접적인 영향을 미치는 이슈들이기 때문이다. 위에서 언급한 ‘새로운 포렌식 도구와 기술의 테스트’ 이슈에 대해 모든 국가에서 민간기업 그룹이 상위권으로 나타났으며, 경찰 그룹에서는 중위권으로 나타났다. 그러나 정부 공기업 그룹에서는 미국이 2순위

로 나타났고, 한국과 호주는 각각 8순위와 10순위로 나타났다. 이는 위의 ‘정보의 접근과 획득’ 이슈와 연계하여 설명될 수 있다.

5.2 시사점

본 연구의 시사점은 다음과 같다. 첫째, 디지털 포렌식 분야의 여러 법률적 이슈사항 중 지침 및 표준 확정 시 개발 및 지속적 개선에 기여할 수 있다. 이 필요하다. 현재 국내에 디지털 포렌식 전문가가 매우 적기 때문에 해당 모범 사례 지침과 표준에 대해 개발할 인력이 매우 부족하다. 만약 표준이나 프레임워크를 만든다 할지라도 각 국가의 상황에 맞게 개발 되는 것이므로 국가 경제가 허물어지는 디지털 포렌식의 특성상 매우 비효율적이다. 따라서, 국가간 협력을 통해 각 국가의 특성을 파악하여 모든 국가에 적용할 수 있는 모범 사례와 표준이 개발 되어야 함을 판단할 수 있었다. 또한 각 국가의 특성 혹은 현 디지털 포렌식 분야의 현황을 파악하는 데 본 연구의 결과가 반영될 수 있을 것이라 판단할 수 있었다. 각 국가는 디지털 포렌식 분야에 적용되는 이해관계자이자 전문가를 모집해 해당 표준에 대해 개발하고 지속적으로 검토 및 개선 활동을 해 나가야 하기 때문이다. 둘째, 국내 디지털 포렌식 분야에서 법률적 이슈사항에 대한 우선순위 연구의 그 기반으로 향후 우선순위가 높은 이슈들에 대한 연구의 시발점이 될 수 있을 것이다. 본 연구를 통해 국내에서 ‘모범 사례 지침과 표준의 필요성’, ‘정보의 접근과 획득’, ‘법률 종사자들의 디지털 증거 이해능력’ 등 우선순위가 높은 이슈를 파악할 수 있었고 이에 대한 구체적인 연구의 우선순위를 파악할 수 있었다. 특히, 국가와 그룹의 구분없이 높은 우선순위가 나온 ‘정보의 접근과 획득’은 각 국가 별 연구 동향을 파악하며 연구를 한다면 좀 더 좋은 연구가 될 것으로 판단할 수 있다. 셋째, 디지털 포렌식 분야에서의 법률적 이슈사항에 대한 우선순위 연구 방법을 체

계화 할 수 있었다. 기존의 Brungs-Jamieson(2005) 연구와 Liles(2009) 연구는 서로 연구방법이 다르고, 필요하지만 생략된 데이터들이 많았다. 향후 타 국가에서 해당 연구를 진행할 시 본 연구의 연구방법을 통해 좀 더 통계적 기법에 따른 체계적인 설득력을 갖춘 연구가 될 수 있을 것이다. 향후 타 국가에서도 동일한 법률적 이슈에 대해 연구를 진행한다면 세계에 통용될 수 있는 디지털 포렌식 분야에서의 표준을 도출하는 데 핵심적 역할을 할 수 있을 것이다.

5.3 한계점 및 향후 연구방향

본 연구는 디지털 포렌식이라는 생소한 분야 내 여러 이해관계자 간의 관계, 국가 간 공통된 이해관계를 파악하고 이끌어내기 위한 연구라는 점에서 학술적, 실무적 의의가 있지만, 본 연구의 인터뷰 대상이 디지털 포렌식 종사자라는 특성상, 샘플 확보에 어려움을 겪어 표본수가 많지 않았고 그룹 별 샘플 수가 동일하지 않으며, 법조계 종사자와 학계 종사자들에 대해 설문은 수행하지 못했다는 점, 선행연구 간 다른 연구방법과 샘플 수로 인해 명확한 비교가 힘들었다는 점을 본 연구의 한계점으로 들 수 있다. 해당 문제점은 추후 디지털 포렌식 분야의 표준 도출 연구를 진행하면서 보완될 수 있을 것이다.

참고 문헌

- [1] 광병선, “디지털 포렌식 수사의 문제점과 개선 방안”, *법학연구*, 제42권, 2011, pp. 171-191.
- [2] 권양섭, “형사절차상의 디지털 증거개시(E-Discovery) 제도에 관한 고찰”, *법학연구*, 제62호, 2016a, pp. 421-442.
- [3] 권양섭, “유비쿼터스 컴퓨팅환경하에서 디지털 포렌식 수사절차에 관한 연구”, *법학연구*, 제16권, 제1호, 2016b, pp. 93-120.
- [4] 권영욱, 김병도, “정보보안 사고와 사고방지 관련 투자가 기업가치에 미치는 영향”, *Information Systems Review*, 제9권, 제1호, 2007, pp. 105-120.
- [5] 김민석, 박석천, “홈오토메이션 환경에서 디지털 포렌식 보안 방식 제안”, *한국인터넷정보학회 학술발표대회 논문집*, 2015, pp. 277-278.
- [6] 김승용, 김상욱, 황인철, “기업 보안을 위한 CCTV 비활당 영역 분석용 디지털 포렌식 솔루션 개발”, *인터넷전자상거래연구*, 제16권, 제4호, 2016, pp. 185-202.
- [7] 대검찰청, *디지털 증거의 무결성 유지를 위한 절차와 시설에 관한 연구*, 대검찰청, 2006.
- [8] 대검찰청, *디지털 증거의 압수수색과 증거능력 제고 방안*, 대검찰청, 2014.
- [9] 박세환, *디지털 포렌식 기술 동향 및 국내 경쟁력*, 정보통신산업진흥원, 2015.
- [10] 박종성, 문종섭, 최운호, “자동화된 침해사고 대응시스템에서 네트워크 포렌식 정보에 대한 정의”, *정보보호학회지*, 제14권, 제4호, 2004.
- [11] 백승조, 심미나, 임종인, “국가 디지털 포렌식 법률 체계와 국내외 디지털 포렌식 법적 현황”, *정보보호학회지*, 제18권, 제1호, 2008, pp. 49-61.
- [12] 성혜정, 유혜정, “디지털 증거 검증기관의 역할 및 처리절차에 대한 연구”, *한국정보기술학회논문지*, 제12호, 제7권, 2014, pp. 79-88.
- [13] 신지호, 최낙범, “경찰 디지털 포렌식 조직구조와 업무과정 개선방안에 관한 연구”, *경찰학연구*, 제16권, 제3호, 2016, pp. 231-262.
- [14] 어수용, 조우연, 이석준, 손태식, “모바일 포렌식 증거능력 확보 방안 연구”, *정보보호학회논문지*, 제26권, 제1호, 2016, pp. 135-152.
- [15] 윤종철, 박용석, “안드로이드 환경에서의 KakaoTalk 메시지의 포렌식 분석 방법론 제안 및 분석”, *한국정보통신학회논문지*, 제20권, 제1호, 2016, pp. 72-80.
- [16] 윤한성, “정보보안 및 정보시스템자산 관리를 위한 내부 감시·통제시스템”, *Information*

- Systems Review*, 제9권, 제1호, 2007, pp. 121-137.
- [17] 이상복, “디지털 포렌식 업무의 법·제도적인 개선방향”, *서강법학*, 제10권, 제2호, 2008, pp. 139-178.
- [18] 이종민, “부산 범죄수사에 디지털 증거분석 의뢰 ‘급증’”, *연합뉴스*, 2013. 01. 06., Available at <http://www.yonhapnews.co.kr/bulletin/2013/01/04/0200000000AKR20130104140100051.HT ML>.
- [19] 이현진, “사이버범죄 10년새 90% 증가...예방 위한 단일 법령 만든다”, *한국경제*, 2017. 4. 20., Available at <http://www.hankyung.com/news/app/newsview.php?aid=2017042057541>.
- [20] 전상덕, 홍동숙, 한기준, “디지털 포렌식의 기술 동향과 전망”, *한국정보사회진흥원*, 제13권, 제4호, 2006, pp. 3-19.
- [21] 정대용, 김성훈, 김기범, 이상진, “국제협력을 통한 디지털 증거의 수집과 증거능력”, *형사정책연구*, 제28권, 제1호, 2017, pp. 49-77.
- [22] 정대회, 이상미, “디지털 증거 압수수색절차에서의 ‘관련성’의 문제”, *형사정책연구*, 제26권, 제2호, 2015, pp. 95-130.
- [23] 조광훈, “디지털 증거의 압수·수색의 문제점과 개선방안”, *서울법학*, 제21권, 제3호, 2014, pp. 699-738.
- [24] 최재민, 이상진, 임종인, “포렌식 어카운팅 기술 동향”, *정보보호학회지*, 제18권, 제1호, 2008, pp. 29-40.
- [25] 탁희성, 이상진, “디지털 증거분석도구에 의한 증거수집절차 및 증거능력 확보방안”, *한국형사정책연구원 연구총서*, 2006, pp. 06-21.
- [26] Broadhurst, R., “Developments in the global law enforcement of cyber-crime”, *Policing: An International Journal of Police Strategies & Management*, Vol.29, No.3, 2006, pp. 408-433.
- [27] Broucek, V. and P. Turner, “Bridging the divide: Rising awareness of forensic issues amongst systems administrators”, In *3rd International System Administration and Networking Conference*, 2002, pp. 27-31.
- [28] Brungs, A. and R. Jamieson, “Identification of legal issues for computer forensics”, *Information Systems Management*, Vol.22, No.2, 2005, pp. 57-66.
- [29] Carney, M. and M. Rogers, “The Trojan made medo it: A first step in statistical based computer forensics event reconstruction”, *International Journal of Digital Evidence*, Vol.2, No.4, 2004, pp. 1-11.
- [30] Chauhan, P. and P. Bansal, “Emphasizing on various security issues in cloud forensic framework”, *Indian Journal of Science and Technology*, Vol.8, No.1, 2016.
- [31] Conley, J. M. and R. M. Bryan, “A survey of computer crime legislation in the united states”, *Information and Communications Technology Law*, Vol.8, No.1, 1999, pp. 35-57.
- [32] Harbawi, M. and A. Varol, “An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework”, In *Digital Forensic and Security(ISDFS)*, *5th International Symposium on IEEE*, 2017, pp. 1-6.
- [33] Laubscher, R., M. S. Olivier, H. S. Venter, D. J. Rabe, and J. H. P. Eloff, “Computer forensics for a computer-based assessment”, *Proceedings of the Fifth Annual Information Security South Africa Conference*, 2005.
- [34] Liles, S., M. Rogers, and M. Hoebich, “A survey of the legal issues facing digital forensic experts”, *IFIP International Conference on Digital Forensics*, Springer Berlin Heidelberg, 2009, pp. 267-276.
- [35] Pocar, F., “New challenges for international rules against cyber-crime”, *European Journal on Criminal Policy and Research*, Vol.10, No.1, 2004, pp. 27-37.
- [36] Reid, L. A., “Amanda M. Hubbard, JD Fulbright

- scholar former trial attorney, computer crime and intellectual property section, US department of justice”, *Journal of Information Privacy and Security*, Vol.2, No.1, 2006 pp. 47-56.
- [37] Reith, M., C. Carr, and G. Gansch, “An examination of digital forensic models”, *International Journal of Digital Evidence*, Vol.1, No.3, 2002.
- [38] Slay, J. and F. Schulz, “Development of an ontology based forensic search mechanism: Proof of concept”, *arXiv preprint arXiv*, 2014, 1407.8258.
- [39] Witter, F., *Legal Aspects of Collecting and Preserving Computer Forensic Evidence*, InfoSec Reading Room, SANS Institute, Bethesda, Maryland, 2001.

〈부 록〉

■ 본 인터뷰는 디지털 포렌식 전문가 분들을 대상으로 합니다.

디지털 포렌식란?

단순히 컴퓨터에서 발생한 범죄의 증거를 수집하는 것뿐만 아니라 증거를 수집하는 과정에서 합법적이고 과학적인 범죄 입증절차를 제시하고 있으며, 과학적인 절차에 의해 수집된 증거를 최종적으로 법원에 제출함으로써 범죄를 증명하는 데 기여하고 있는 분야입니다.

Q. 귀하는 디지털 포렌식에 대한 수사경험 혹은 교육받은 경험이 있으십니까?

예 () 아니오 ()

“아니오”면 설문 중지

1. 다음은 디지털 포렌식 분야에서 법적 이슈사항에 대한 생각을 확인하기 위한 질문입니다.

Q1. “모범 사례 지침과 표준의 필요성”에 대해 어떻게 생각하십니까?

모범 사례 지침과 표준의 필요성이란?

디지털 포렌식 분야에서 디지털 증거의 증거능력을 확보할 수 있도록 절차, 프레임워크 등의 모범 사례들과 표준 확립의 필요성을 의미합니다.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
모범 사례 지침과 표준의 필요성					

Q2. “법률 종사자들의 디지털 증거 이해능력”에 대해 어떻게 생각하십니까?

법률 종사자들의 디지털 증거 이해능력이란?

디지털 포렌식 전문가가 증거로 제출한 디지털 증거에 대해 증거의 정당성과 증거능력을 정확히 파악하기 위해서는 법률 종사자들의 디지털 증거에 대한 이해능력이 필요하다는 것을 의미합니다.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
법률 종사자들의 디지털 증거 이해능력					

Q3. “기업의 기밀에 대한 정보보호”에 대해 어떻게 생각하십니까?

기업의 기밀에 대한 정보보호란?

디지털 증거를 수집할 때, 기업의 기밀 사항이 노출되는 경우가 존재하는데 이에 대한 법, 규정이나 절차가 미비한 것을 의미합니다.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
기업의 기밀에 대한 정보보호					

Q4. “데이터 전송 시 통신 세부정보 보호”에 대해 어떻게 생각하십니까?

데이터 전송 시 통신 세부정보 보호란?
 디지털 포렌식 분야에서 데이터가 실시간 전송 중일 때, 해당 데이터에 대한 보호 법률은 존재하지만 통신 접속 세부정보들에 대해서는 적절한 보호를 받고 있지 못한 데서 발생하는 이슈입니다.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
데이터 전송에 있어서의 프라이버시 보호					

Q5. “형사소송과 민사소송의 차이점”에 대해 어떻게 생각하십니까?

형사소송과 민사소송의 차이점이란?
 형사소송과 민사소송의 차이점에 따른 여러 가지 이슈들에 대해서 발생할 수 있는 문제점들이 존재합니다.
 예) 형사소송 시에는 디지털 증거를 소유하고 있는 사람에게 사전고지 없이 해당 증거를 압수할 수 있음. 민사소송 시에는 디지털 증거를 소유하고 있는 사람이 원고가 찾고자 하는 증거가 무엇인지 알 수 있기 때문에 해당 증거에 대한 위·변조 혹은 파기가 가능함.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
형사소송 대 민사소송의 차이점					

Q6. “감시와 프라이버시”에 대해 어떻게 생각하십니까?

감시와 프라이버시란?
 디지털 증거를 수집하기 위해 CCTV, 개인의 접속기록, 개인정보 등에 대해 무차별적으로 수집하는 것에 대해 범위 제한이나 절차가 충분히 않은 것에 대한 이슈입니다.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
감시와 프라이버시					

Q7. “디지털 증거에 영향을 미치는 법의 해석”에 대해 어떻게 생각하십니까?

디지털 증거에 영향을 미치는 법의 해석이란?
 통신 세부정보사항에 있어서 언제가 통신의 시작과 끝을 의미하는지, 언제가 이메일을 읽고 읽지 않음을 세부적으로 구분하는지에 대한 불확실한 상황에 대해 법적으로 명확화 한 것이 없습니다. 이에 따라 해석의 다양성이 존재하는 것에 대한 이슈입니다.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
디지털 증거에 영향을 미치는 법의 해석					

Q8. “정보로의 접근과 획득”에 대해 어떻게 생각하십니까?

정보로의 접근과 획득이란?
 디지털 증거를 확보하기 위해 통신회사나 ISP에 협조를 요청할 필요가 있습니다. 그러나 정보의 범위와 그 수준과 관련된 법률이 존재하지 않아 디지털 증거에 대한 접근과 확보가 어려운 것에 대한 이슈입니다.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
정보로의 접근과 획득					

Q9. “법률 부문에서의 국제협력”에 대해 어떻게 생각하십니까?

법률 부문에서의 국제협력이란?
 디지털 증거의 특성 상 국가 경계를 넘나들기 때문에 디지털 증거를 수집하기 위해 국가 간 협력이 필요할 때가 존재합니다. 이에 대해 각 국가의 제정법이 다르므로 수사 시 협력할 수 있는 표준이 필요하다는 것에 대한 이슈입니다.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
법률 부문에서의 국제협력					

Q10. “디지털 증거 조사 중 개인의 프라이버시 보호”에 대해 어떻게 생각하십니까?

디지털 증거 조사 중 개인의 프라이버시 보호란?
 디지털 증거 수색 과정 시 범죄 관련 내용과 관련없는 부분의 노출에 대해 범위의 규정이나 법적 규제가 존재하지 않음에 대해 생기는 이슈입니다.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
디지털 증거 조사 중 개인의 프라이버시 보호					

Q11. “디바이스에 따라 적용되는 법의 종류”에 대해 어떻게 생각하십니까?

디바이스에 따라 적용되는 법의 종류란?
 디지털 포렌식 분야는 컴퓨터, 스마트폰, TV, IPTV 등 다양한 디바이스에 대해 이루어집니다. 각 매개체에 따라 적용되는 법이 다르므로 이에 대해 발생하는 여러 이슈들이 존재합니다.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
방송과 정보통신의 대조					

Q12. “새로운 위법행위를 구체화할 필요성”에 대해 어떻게 생각하십니까?

새로운 위법행위를 구체화할 필요성이란?
 디지털 포렌식 분야에서 앞으로 발생할 새로운 분야의 사건들에 대해 정확히 파악하여 구체화하지 않는다면 해당 범죄가 발생하더라도 명확한 원인 파악과 증거 추출이 힘들어지고 해당 법이 존재하지 않아 처벌이 힘들어지는 것에 대한 이슈입니다.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
새로운 위법행위를 구체화할 필요성					

Q13. “민간 기업의 증거 수집”에 대해 어떻게 생각하십니까?

민간 기업의 증거 수집이란?
 민간 기업에서 디지털 범죄가 발생했을 때 증거를 수집하여야 하는데 여기서 발생하는 ‘사건과 관련된 디지털 증거가 어떠한 것인가?’, ‘이 증거가 어디에 존재하는가?’, ‘이 증거를 누가 관리하고 있는가?’ 등 다양한 문제점에 대해 해결할 필요가 있다는 것을 의미합니다.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
민간 기업의 증거 수집					

Q14. “새로운 포렌식 도구와 기술의 테스트”에 대해 어떻게 생각하십니까?

새로운 포렌식 도구와 기술의 테스트란?
 디바이스의 다양화와 기술의 발전은 앞으로 다양한 범죄를 불러일으킵니다. 그에 따라 기존의 포렌식 도구와 기술의 발전 및 새로운 도구 개발을 지속하고 검증해야 한다는 것을 의미합니다.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
새로운 포렌식 도구와 기술의 테스트					

Q15. “전문가로서의 진술 능력과 자격 요건”에 대해 어떻게 생각하십니까?

전문가로서의 진술 능력과 자격 요건이란?
 디지털 증거가 법정에서 효력이 있게 하는 것은 전문가의 진술 능력과 자격 요건입니다. 판결에 있어서 매우 중요한 부분이므로 이에 대한 최소한의 기준 확립이 필요하다는 것을 의미합니다.

	전혀 중요치 않음	중요치 않음	보통	중요함	매우 중요함
전문가로서의 진술 능력과 자격 요건					

2. 다음은 법률적 이슈사항에 대한 우선순위를 확인하기 위한 질문입니다.

(각 항목별로 1~15까지 중복되지 않도록 숫자를 기입해주시시오. 1부터 15까지 하나씩 모든 숫자가 포함되어야 합니다. 1은 ‘가장 중요함’, 15는 ‘가장 덜 중요함’을 의미합니다.)

법률적 이슈사항	순위
모범 사례 지침과 표준의 필요성	
법률 종사자들의 컴퓨터 이해능력	
기업의 기밀에 대한 프라이버시	
데이터 전송에 있어서의 프라이버시 보호	
형사소송 대 민사소송	
감시와 프라이버시	
디지털 증거에 영향을 미치는 법의 해석	
정보로의 접근과 교환	
법률 부문에서의 국제협력	
디지털 증거 조사 중 개인의 프라이버시 보호	
방송과 정보통신의 대조	
새로운 위법행위를 구체화할 필요성	
비정부 조직이 증거를 수집할 때 발생하는 문제점	
새로운 포렌식 도구와 기술의 테스트	
전문가로서의 진술 능력과 자격 요건	

위의 표에서 가장 중요하다고 생각하는 항목(1순위)에 대해 선정하신 이유는 무엇입니까?
()

위의 표에서 가장 중요하지 않다고 생각하는 항목(15순위)에 대해 선정하신 이유는 무엇입니까?
()

▣ 귀하의 인적 사항에 대한 질문입니다.

1. 성별:

① 남 ② 여

2. 나이: 만 () 세

3. 직업:

① 경찰 ② 정부 & 공공기관 ③ 학계 종사자 ④ 직장인 ⑤ 법률 종사자 ⑥ 기타 ()

4. 학력:

① 대학원 졸업 ② 대학 졸업 ③ 전문대학 졸업 ④ 고등학교 졸업 ⑤ 기타 ()

▣ 모든 인터뷰가 종료되었습니다. 참여해 주셔서 대단히 감사합니다.

A Study for Comparing the Legal Importance of Digital Forensics Issues in Korea

Jae Bin Lee* · Won Kyung Sung** · Choong C. Lee***

Abstract

In modern society, crime records have been digitized. Digital information is difficult to distinguish from original information, but the former is easy to modulate. This situation explains the increasing importance of digital forensics. However, digital forensic has several inefficiencies because of the rapid development of technology, unclear jurisdiction, and tool errors. This study surveyed digital forensic specialists and derived the priority of domestic digital forensic issues by redefining 17 issues in digital forensics from Brungs-Jamieson study in Australia. The present study was divided into four groups, namely, police, government and public corporations, private companies, and legal groups. The study could compare and analyze comparative analysis of existing studies in Australia and the US. This study can also examine differences in the results of each group in Korea. Thus, the key issues in Korea were derived as “Requirements to ‘Fire Up’ Original.” The differences of the three groups in terms of legal issues were then identified. This finding enables us to understand differences in priorities and importance between groups and countries.

Keywords: *Digital Forensic, Legal issues, Priority*

* AhnLab, Inc.

** Graduate School of Information, Yonsei University

*** Corresponding Author, Graduate School of Information, Yonsei University

◎ 저 자 소 개 ◎



이 재 빈 (jaebin.lee@ahnlab.com)

연세대학교에서 컴퓨터공학 학사를 마쳤으며, 연세대학교 정보대학원에서 지식 서비스보안트랙을 전공하여 석사학위를 취득하였다. 현재 Ahnlab에서 보안 컨설턴트로 재직 중에 있으며, 주요 관심분야는 Security Architecture, System Hacking, Web Hacking 등이다.



성 원 경 (sung_wonkyung@yonsei.ac.kr)

가톨릭대학교에서 문화 콘텐츠학과에서 학사를 마쳤으며, 현재 연세대학교 정보대학원 정보시스템학 비즈니스 빅데이터 분석 트랙 석사를 이수 중에 있다. 주요 연구 관심분야는 Data Mining, Deep Learning의 CNN과 LSTM을 활용한 이미지 처리, 및 텍스트 분석 분야이다.



이 중 정 (cclee@yonsei.ac.kr)

University of South Carolina에서 MIS를 전공하여 박사학위를 취득하였다. 이후 미국 Salisbury에 있는 메릴랜드 주립대학교의 교수로 재직한 바 있으며, 현재 연세대학교 정보대학원의 교수로 재직 중이다. MIS Quarterly, Journal of Management Information Systems, Decision Sciences, Communications of ACM 등의 국제 주요 학술지 및 APJIS(경영정보학연구) 등의 국내 학술지에 논문을 게재한 바 있다. 주요 연구 관심분야는 IT Performance, IT Evaluation Measurement, Information Orientation 등이다.

논문접수일 : 2017년 04월 30일

게재확정일 : 2017년 07월 04일

1차 수정일 : 2017년 06월 28일