연구보고서 2008-00

경찰의 차세대 디지털 포렌식 기반 구축방안

≪硏 究 陣≫

연 구 위 원 : 임 종 인 (고려대학교 정보경영공학전문대학원)

목 차

표 목 차

그 림 목 차

제1장 서 론

제1절 연구목적

최근 디지털 증거를 다루는 법과학(Forensics)이라고 할 수 있는 디지털 포렌식이 전 세계 법집행기관에 중요한 화두로 대두되고 있다. 디지털 증거를 통해 범죄를 해결해야 할 필요성이 뚜렷해진 반면에 법률이나 제도, 혹은 기술적으로 이 문제에 적절히 대처하기 위해 넘어야할 난관이 매우 크기 때문이다. 이러한 문제점을 간파한 미국 등 선진국은 이미 1990년대 초반부터 이 분야에 대한 발전을 위해 막대한 예산을 투자하여 탄탄한 기반을 구축해 나가고 있으며 국내에서도 2000년대 초반부터 법과학으로서 디지털 포렌식에 대한 인식을 새로이 하고 노력을 기울이고 있다. 특히 2004년 경찰청 디지털 포렌식센터의 설치와 같은 법집행기관 내부의 발전, 2005년 한국디지털포렌식 학회의 창립과 같은 학계의 발전과 아울러 법조계나 유관기관에서의 다양한 관심과 노력이 뒤를 잇고 있다.

법과학은 한 나라의 선진화된 사법서비스의 필수적 요소이자 관련된 전문인력의 교육, 고용이나 제품이나 기술 등 막대한 경제적 가치를 지닌 하나의 산업이다. 따라서 그 비중이 급격히 증가하고 있는 디지털 포렌식을 발전시키는 것은 단지 수사기관의 필요가 아니라 국가적인 과제로 인식되어야 마땅하다. 이를 위해서는 관련되는 법률이나 제도, 기술 등 여러 측면에서 사회적인 공감대의 형성과 공동 혹은 각 참여기관이나 개인의 노력이 수반되어야 한다.

하지만 미국 등 선진국의 디지털 포렌식이 오랜 기간 축적되어 온 법과학의 여러 제도적 기반 하에 컴퓨터 관련 범죄의 발생 초기부터 점진적이고 체계적으로 이루어진 반면, 국내에서는 상대적으로 열악한 법과학 내지 과학수사의 환경 하에서 기술을 중심으로 급격하게 디지털 포렌식이 도입되었기 때문에 아직 법률이나 제도, 운영, 기술 등 여러 측면에서 기반이 탄탄하다고 보기 어렵다. 그 원인으로는 무엇보다 디지털 포렌식을 구성

하는 각 구성요소들은 각기 독립된 것이 아니라 상호 긴밀하게 관련되어 있음에도 불구하고 그 전체를 아우르는 체계와 방향성에 대한 공감대가 형성되지 않아 각 구성요소간의 조화와 발전의 균형을 이루지 못하고 있음을 들 수 있다.

이에 본 연구에서는 향후의 디지털 포렌식은 여러 하위요소들을 구분, 요소별 요구와 요소간의 조화를 바탕으로 하나의 시스템적 체계를 지녀야 한다는 인식하에 경찰과 관련된 분야를 중심으로 디지털 포렌식의 선진적 발전 방향을 모색하고자 한다.

제2절 연구내용과 방법

1. 연구내용

먼저 제2장에서 디지털 포렌식 체계에 대한 분석적 접근을 위해 디지털 포렌식의 의의와 간략하게 발전경과를 살펴보고 그 결과로서 개괄적인 접근방향에 대한 개념적 구조화를 법, 운영, 기술적인 측면으로 구분하여 접근하였고 구체적, 실천적인 측면에서 디지털 분야에 한정하지 않고 전체로서의 법과학의 기반을 구성한다고 볼 수 있는 요소들을 중요하다고 생각되는 사항들만 정리하였다.

다음으로 디지털 포렌식이 선진적 형태를 갖추기 위해서는 이 분야가 발전해 온 여러 측면에서의 경과와 방향을 인지하는게 우선되어야 할 것이다. 각 국가의 법률과 제도가 다르기는 하지만 특히 디지털 포렌식 분야는 국제적인 보편성과 표준을 중시하기 때문에 이러한 측면에서 선진 디지털 포렌식 체계의 발전 상황을 살펴볼 필요가 있다. 특히, 여러 국가의 제도를 상호비교하기 보다는 이 분야에 대한 발전을 국제적으로 선도하고 있다고 볼 수 있는 미국의 체계를 심층적으로 분석하여 발전의 틀을 형성하고있는 맥락을 발견하려고 하였다. 이를 통해 디지털 포렌식 체계의 하위 요소들을 구분하고 각 요소별 발전과 요소간의 조화가 어떻게 이루어져야 하는 지에 대해 살펴보았다.

이어서 앞에서 발견된 디지털 포렌식 체계의 틀에 맞추어 경찰을 중심으로 국내의 디지털 포렌식 체계의 현황을 살펴보았다.

신기술에 대한 개발수요와 추세는 국내외를 구분하기 보다는 장을 분리하여 그 다음에 정리하였다.

끝으로 디지털 포렌식 체계의 하위 요소에서 나타나는 개별적인 문제점을 한·미간의 비교적 관점에서 종합적으로 분석하여 향후 디지털 포렌식의 발전방향을 모색하고 이를 해결하기 위한 과제들을 탐색하였다.

2. 연구방법

광범위한 내용에 대한 전반적인 측면에서의 접근을 필요로 하는 연구주제의 특성상 개별적인 주제 전체에 대한 심층적인 조사연구보다는 각 부분의 특징적 요소와 요소간의 관계를 분석·기술하는데 우선을 두었다.

외국의 사례는 관련 문헌과 각 기관 등의 웹사이트의 자료를 수집하여 분석하였으며 부분적으로 직·간접적으로 수사관 등 실무자에 대한 면담이나 수사관간의 세미나 등에서 언급된 자료들을 참고하였다. 국내 자료는 선행연구 자료들이 주로 기술적 측면에서 집중되어 있어 분석자료가 부족한 아쉬움이 많았다. 경찰청으로부터 일부 자료를 제공받아 분석하였으며, 현직 경찰관의 디지털 포렌식에 대한 인식에 대한 설문조사를 실시하였다.

디지털 증거분석 현황 등에 대해서는 실제 디지털 증거분석 자료에 대한 직접적인 열람으로 야기될 수 있는 문제점 등을 고려하여 현직 경찰 신분인 연구참여자가 전담하여 분석하였다. 또한 실무 현장에서의 디지털 증거처리의 업무관행 등 조사가 곤란한 부분에 대해 수사관들과의 면담 등을 통해 현황을 파악하였다. 따라서 그러한 부분이 포함된 내용의 일부는 다소 경험적일 수밖에 없는 한계가 있다고 할 수 있다.

3. 연구결과의 활용

본 연구는 무엇보다 경찰청에서 디지털 포렌식과 관련된 정책의 수립에 참고자료로 사

용될 수 있을 것이다. 경찰청 전체 차원에서는 이를 통해 디지털 포렌식의 중요성에 대한 인식과 함께 이 분야에 대한 예산의 배분이나 인력의 모집과 배치와 같은 여러 측면에서의 배려가 이루어질 것으로 기대하고 있으며, 담당 부서에서는 장·단기의 정책의 수립과 집행, 각 정책에 있어 우선순위의 결정에 참고가 될 것이다.

한편으로 디지털 포렌식이 단지 수사기관의 전유물이 아닐 뿐 아니라 수사기관의 입장에서도 이와 관계되는 정부부처 및 학계, 산업계에서의 지원을 필요로 하며, 무엇보다 디지털 포렌식이 국가적인 차원에서 발전을 도모해야 한다는 측면에서 상호간의 이해와 협력에 본 연구가 다소간 도움이 될 것으로 기대된다.

제2장 유비쿼터스 시대 경찰의 과제와 디지털 포렌식

제1절 서 설

인류는 정보통신기술(Information and Communication Technology, ICT)의 개발로 농경사회는 물론 산업사회의 발달보다도 더 짧은 기간 안에 더 극적인 변화를 겪었고 그 변화는 지금도 빠른 속도로 진행되고 있다. 이러한 변화는 경찰 등 법집행기관에게도 예외가 아니다. 인터넷을 통해 범죄를 신고 받고 각종 통신장비를 이용하여 범인을 추적하거나 교통을 단속하며, 정보를 수집하여 데이터웨어하우스를 구축하고 데이터마이닝이나 지리적 프로파일링 등의 분석을 위해 수많은 정보통신기기와 기술을 활용하는 것은 현대 법집행기관에 있어 일상이 되고 있다.

한편 범죄자들에게도 정보통신기술은 새로운 범죄의 기회를 제공하고 있다. 이러한 범죄는 사기, 명예훼손, 협박, 지적재산권의 침해 등 정보통신망을 전통적 범죄를 실행하는데 범행실행의 주된 혹은 보조적인 도구로 사용하는 것 뿐 아니라 해킹이나 악성프로그램의 유포와 같은 컴퓨터 시스템이나 네트워크 자체를 공격대상으로 하는 것까지 다양하다. 정보통신망을 이용하는 범죄행위들은 자동성, 원격성, 기술보급과 같은 특성[1]들로 인해 범죄의 예방 뿐 아니라 범죄혐의를 발견하고 증거를 수집하여 범죄자를 검거하는 각 수사단계에서 많은 어려움이 있다. 따라서 이에 대응하기 위해 각국의 국가적, 국제적인 노력이 진행 중이다.

그 뿐 아니라 이제 정보통신기술을 범죄도구나 대상으로 사용하지 않는 범죄라고 하더라도 범죄수사를 위해 디지털 정보를 다루는 일은 필수적인 것이 되었다. 미국 버클리대학의 한 조사[2]에 따르면 2002년 전 세계에서 생산되는 모든 정보의 약92%가 하드디스크 등 전자기적 매체에 저장되고 있다고 하니 디지털 CCTV나 휴대전화 추적과 같은 디지털 정

1) Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World, John Wiley & Sons,* 2000, pp.17-22.

2) http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm 참조. 이하 모든 인용된 웹사이트는 2007. 11. 30. 기준으로 링크의 유효함과 인용된 내용의 변동 없음을 확인하였음.

보를 다루는 수사활동이 증가하는 것은 당연하다고 하겠다. 미국의 경우 모든 범죄사건의 80 내지 90 퍼센트에서 디지털 증거가 포함된다고 하는 추정치가 제시되기도 했다.[3)]

이에 위와 같은 범죄들을 수사하기 위해 디지털 증거를 다루는 법과학의 한 분야인 디지털 포렌식이 법집행기관의 주요한 수사방법이자 법정에서 진실발견의 주요한 도구로 크게 주목받고 있다. 하지만 디지털 증거는 종전의 물리적인 증거나 생물학적인 증거들, 혹은 문서와 같은 증거들과는 구별되는 또 다른 특성을 지니며 이에 따라 법적, 기술적인 문제를 포함하여 법집행기관에 수많은 과제를 제시하고 있다.

게다가 최근의 디지털 증거와 관련된 범죄수사 환경은 매우 급격한 변화를 겪고 있다. 위법수집 증거의 배제법칙을 명문화하고 일반시민이 공판에 참여하며 수사절차의 엄격성을 더한 형사소송법이 개정되어 종래의 수사관행에 큰 변화가 불가피하게 되었다. 시민들은 경찰이 외국의 범죄현장 수사드라마에서 보는 것과 같은 좀 더 과학적인 수사방법을 사용할 것을 요구하고 있다. 디지털 증거가 수집되는 정보통신망은 유비쿼터스 시대를 맞아 이동성과 다양성, 복합성이 크게 증가하고 있다.

이러한 문제들에 대처하기 위해 법집행기관은 조직을 개편하고 전문인력을 모집, 훈련시키고 관련 기술을 개발하는 등의 다각적인 대응노력을 기울이고 있다. 이른바 디지털 포렌식 체계를 구축하는 것이다. 법과학 체계의 수준은 한 국가의 사법체계의 수준과 동일시된다. 그것은 법과학의 수준이 단순한 기술적인 문제가 아니라 이와 관련된 법과 제도, 사회·문화와 같은 수많은 요인과 상호작용하는 하나의 거대한 구조이기 때문에 소수의 인원에 의해 단시간 내에 발달하기 어려운 것이기 때문에 더욱 그렇다. 따라서 앞으로도 지속적으로 증가할 디지털 포렌식 수요를 감당할 충분한 역량을 보유하는 것은 국가적으로 매우 중요한 과제라고 할 수 있다.

제2절 디지털 포렌식의 개념과 분류

법과학(Forensic Science), 혹은 Forensics는 흔히 과학을 법에 응용하는 것[4)]이라

3) K. Meadaris, "*Grants to help develop ways to improve digital evidence collection*", Purdue University, http://www.purdue.edu/UNS/html4ever/2006/061012RogersGrant.html, Oct. 2006.

고 하며, 이에는 사법제도에서 응용되는 모든 과학(science)과 기예(art)를 포괄한다. 이에 따르면 디지털 포렌식은 디지털과 관련된 과학과 기예를 법적 절차에 응용하는 것을 의미한다. 과학은 자연현상이나 사회현상에 대해 결정론적 관점에서 그 원리를 알아내어 이론을 수립하는 것으로 경험에 의해 개발되고 비법과 숙련을 통해서 전수되는 'technique'과 'technique'에 대한 체계적인 이론연구를 하는 'technology' 및 이것들을 이용하여 제품을 만들어 내는 'engineering'과는 각각 구별된다[5].

자연과학이 이론적이며 순수한 지식에 주된 관심이 있다면 법과학은 실용적이며 자연과학의 지식을 응용하는 것이다[6]. 실제로 포렌식스(Forensics)는 이론과 지식 자체 뿐 아니라 그 목적을 달성하기 위해 사용되는 기술과 그것을 가능하게 해주는 제도나 방법 등 환경을 모두 고려하여야 한다. 어떠한 분야가 과학(science)인지 기술(technique)인지를 구별하는 문제 혹은 무엇이 과학적이고 무엇이 과학적이지 않은 지를 구분하는 문제(구획문제, demarcation problem)는 법과학에서 흔히 다루어지는 논란거리이며 결코 쉽지 않은 문제이다.

따라서 이러한 개념 정의보다는 좀 더 구체적으로 디지털 포렌식을 '법적으로 받아들여질 수 있는 방법으로 디지털 증거를 식별(identifying), 보존(preserving), 분석(analyzing), 제출(presentation)하는 과정(process)[7]'이라거나 '범죄에 관한 사건의 재구성이나 계획된 작업에 해를 가하는 인가받지 않은 행위에 대한 예측을 가능하게 하기 위한 목적으로 디지털 소스로부터 추출한 디지털 증거를 보존(preservation), 수집(collection), 검증(validation), 식별(identification), 분석(analysis), 해석(interpretation), 문서화(documentation), 제출(presentation)하는 과학적으로 도출되고 증명된 수단의 이용[8]'과 같이 일련의 프로세스 모델을 기반으로 하여 설명하는 것이 보다 일반적이다.

---

4) R. Saferstein, *Criminalistics: An instruction to forensic science 9th Edition*, Pearson Prentice Hall, 2007. p.4.
5) J. Ladyman(박영태 옮김), 과학철학의 이해, 이학사, 2003, 22면.
6) J. Stuart and J. Nordby, *Forensic Science: An Introduction to Scientific and Investigative Techniques,* CRC, 2002. p.6.
7) R. McKemmish, *What is Forensic Computing? Australian Institute of Criminology Trends and Issues 118*. 1999, (http://www.aic.gov.au/publications/tandi/ti118.pdf)
8) G. Palmer, *"A Road Map for Digital Forensic Research. Technical Report DTR-T0010-01"*, DFRWS, November 2001. Report from the First Digital Forensic Research Workshop (DFRWS). p.16.

한편 컴퓨터 포렌식, 네트워크 포렌식, 포렌식 컴퓨팅, 인터넷 포렌식 등 다양한 용어가 디지털 포렌식과 흔히 혼용되곤 한다. 후술하는 바와 같이 컴퓨터 포렌식은 다양한 매체에 대한 수용가능성의 필요를 토대로 디지털 포렌식이라는 용어로 점차 변화해왔고, 네트워크 포렌식은 정보보호 커뮤니티에서 주로 사용하는 용어이며, 포렌식 컴퓨팅은 컴퓨터과학적 측면을 인터넷 포렌식은 인터넷 이용과 관련된 측면을 각각 강조한 용어라고 할 수 있다. 현재로서는 이 전체 포괄할 수 있는 용어로 디지털 포렌식을 사용하고자 한다.

디지털 포렌식은 매우 다양한 형태로 분류될 수 있다. 아직 디지털 포렌식의 분류에 대해서는 국제적으로 통일된 기준이 마련된 것으로 보이지 않는다. 아래의 표[9]는 수많은 분류방법 중의 하나일 따름이나, 이를 통해 보는 관점에 따라 디지털 포렌식의 분야가 매우 광범위하게 분류될 수 있음을 보여준다.

<표 1> 디지털 포렌식의 분류

응용 프로그램 관점	인터넷 브라우저 포렌식
	이메일 포렌식
	레지스터 파일 포렌식
	응용프로그램 포렌식
	바이러스 포렌식
	웜 포렌식
	File slack, Erased files and Swap files
시스템 관점	유닉스 시스템 포렌식
	윈도우 파일 시스템 포렌식
	로그 시스템 포렌식
	감사 시스템 포렌식
하드웨어 관점	PC 포렌식
	PDA 포렌식
	프린터 포렌식
	라우터 포렌식
	방화벽 포렌식
과정(process) 관점	피해자측 포렌식
	중간매개자측 포렌식
	공격자측 포렌식

9) W. Ren, "*Modeling Network Forensics Behavior*", Journal of Digital Forensic Practice 1:57-65.

제3절 디지털 포렌식의 역사

1. 컴퓨터 포렌식의 태동기 (1980년대 ~ 1990년대 중반)

디지털 증거에 대한 인식은 컴퓨터 범죄의 발생에 대처하기 위한 수사 혹은 정보기관의 노력에서 비롯되었다고 볼 수 있다. PC가 보급되기 이전에도 은행에서의 잔전 빼돌리기(salami slicing)와 같은 컴퓨터 범죄가 없었던 것은 아니지만 복잡한 메인프레임(main frame) 컴퓨터에서 증거를 추출하는 것은 대부분의 컴퓨터를 다루어보지 않은 수사관에게 쉬운 일이 아니었다. 1980년대 PC 보급 이후에는 "X-Tree Gold"나 "Norton Disk Edit" 등의 파일 관리 도구를 이용하여 간단한 파일 복구 작업이 수사에 활용되었으나 당시의 디지털 수사는 마치 컴퓨터에 관심이 많은 수사관의 취미활동과 같은 것이었다.

1984년 미연방수사국 FBI는 자기매체프로그램(Magnetic Media Program)을 통해 컴퓨터 증거분석에 대한 공식적인 대응을 시작했으며 이것은 추후 컴퓨터분석대응팀(Computer Analysis and Response Team)으로 발전하게 된다. 1988년 미국 국세청 IRS의 Michael Anderson은 이 분야에 관심이 있는 수사관과 법률가, 업체 관계자들과의 정기적인 만남을 가졌으며 곧 연방법집행훈련센터(FLETC)에 최초로 컴퓨터증거분석전문가 과정을 개설하였고 이러한 모임은 1991년 수사관을 주축으로 한 대규모 모임인 International Association of Computer Investigative Specialists(IACIS) 창설의 모태가 된다. 미국 Portland에서 열린 IACIS모임에서는 처음으로 "Computer Forensics"라는 용어가 사용된 것으로 알려져 있다.[10]

비슷한 시기에 첨단범죄수사협회(High Technology Crime Investigation Association) 등 유사한 자발적 조직들이 결성된다. 1992년 수사기관의 요청을 받은 소프트웨어 업체인 ASR Data에서 파일복구 기능을 지닌 최초의 포렌식 전용 프로그램인 "Expert Witness"를 출시하였다. 당시 이 작업의 파트너 중 일부가 회사를 떠나 현재 전 세계에서 가장 흔히 사용되는 디지털 포렌식 도구인 "Encase"를 만들었다. 이후 컴퓨터 포렌식은 상당기간 정

10) 임종인, "유비쿼터스 시대의 컴퓨터 포렌식의 중요성과 향후 전망", 수사연구 2005년 3월호:12-16, 12면.

제된 이론적 토대없이 주로 포렌식 업계와 이를 응용한 기술에 의해 주도되었다[11]. 1990년 미 Postal Inspection Service Laboratory는 컴퓨터 포렌식 부서를 설치하였다.

2. 컴퓨터 포렌식의 확산기 (1990년대 중반 ~ 2000)

1990년 중반 인터넷이 일반에 보급되기 시작하면서 컴퓨터 증거의 중요성에 대한 인식은 법집행기관 내외에서 좀 더 널리 확산되게 된다. 1993년 FBI는 70개 국내외 기관 대표가 참여한 가운데 1차 International Conference on Computer Evidence를 주최하였다. 몇 차례에 걸친 이 컨퍼런스에서의 주된 관심사는 컴퓨터 포렌식의 표준이 필요하다는 것이었고, 결국 이는 International Organization on Computer Evidence(IOCE)의 결성으로 이어지게 되었다. 1998년에는 INTERPOL Forensic Science Symposium이 결성된다.

1998년 워싱턴 지역의 연방 연방의 포렌식랩[12] 책임자들의 정기적인 모임에서 당시에 컴퓨터 외에 비디오와 오디오 증거가 급격히 디지털화되면서 이를 포괄하는 용어로 디지털 증거에 대한 용어의 채택가능성을 논의했으며 결국 다른 많은 기관의 동참하에 Scientific Working Group Digital Evidence(SWGDE)[13]의 결성으로 이어진다. SWGDE의 주된 관심사는 포렌식랩을 어떻게 세팅하는 것이었으나 그 일부분으로 1999년 디지털 증거 처리에 관한 일련의 준칙(principles)과 정의(definition)을 정하게 되었고, 영국의 United Kingdom's Association of Chief Police Officers(ACPO)의 Best Practice Guide와 함께 IOCE의 준칙의 근간을 이루게 된다. IOCE의 준칙은 다

11) M. Rogerts and K. Seigfried, "*The Future of Computer Forensics: a needs analysis survey*", Computers & Security (2004) 23:12-16, p.13.

12) 포렌식랩(Forensic Laboratory)은 Crime Laboratory, Police Laboratory 등으로 불리며 국내에서는 법과학 시험기관, 법과학연구실 혹은 실험실 등 다양한 명칭으로 불리고 있다. 여기에서는 한글화된 명칭이 그다지 직관적이지 못하다고 생각되므로 포렌식랩이라는 용어를 사용한다.

13) SWGDE의 최초 명칭은 Technical Working Group for Digital Evidence(TWGDE)였다(NIJ의 TWGDE와는 구별된다). SWG(Scientific Working Group)은 미국내 법과학계에서 분야별로 표준과 최적의 방법(Best Practice), 프토토콜을 결정하기 위한 전문가들의 집단이다. FBI의 TWG와 구분하기 위해 TWG는 SWG로 명칭이 바뀌게 되며, SWGDE 외에도 Image Technology에 관한 SWGIT가 디지털 포렌식과 깊은 관련이 있다.

시 G-8 Digital Evidence Principle의 기초가 되었다.[14]

1990년대 중반까지 수사기관에서 문제 중의 하나는 디지털 증거를 처리하는데 필요한 자원이 흩어져 있다는 것이었다. 이것은 많은 경우 수사부서에서 디지털 증거에 대한 분석업무를 동시에 수행하는데서 비롯된 것이다. 하지만 점차 이러한 분석업무는 포렌식랩 환경으로 옮겨가게 된다. 1995년 Secret Service의 조사에서 48%의 기관이 컴퓨터 포렌식랩을 보유하고 있으며 수집된 컴퓨터 증거의 68%가 랩의 전문가들에게 전달되었다. 하지만 그 중 70%의 경우에서 이러한 작업이 문서화된 절차 매뉴얼 없이 이루어지고 있다고 한다.[15] 1999년 미국 FBI는 FBI 자체 사건에서의 디지털 증거처리를 전담하는 Computer Analysis and Response Team(CART)를 창설하고, 2000년부터 각 지역을 기반으로 관할 내의 법집행기관에 디지털 포렌식 서비스를 제공하는 Regional Computer Forensics Laboratory(RCFL)을 설치 운영하고 있다.

3. 디지털 포렌식의 정착기 (2000년대 이후)

SWGDE는 American Society of Crime Laboratory Directors(ASCLD)와 긴밀하게 협조한 끝에 디지털 포렌식을 정규 법과학 분야로 인식되게 하였으며, 2003년 ASCLD의 랩인증위원회(Laboratory Accreditation Board, ASCLD/LAB)의 인증프로그램의 한 분야로 디지털 및 멀티미디어 증거분야가 채택되었다.

2004년 North Texas RCFL은 최초의 ASCLD/LAB 인증을 받은 연방 디지털 증거 시설이 되었고, FBI OTD (Operational Technology Division)의 Digital Evidence Laboratory(DEL)는 2007. 6 디지털과 멀티미디어 증거(D&ME) 전 분야에서 ASCLD 국제 인증(International Accreditation)을 받은 최초의 랩이 되었다[16]. 다른 연방기관으로는 마약수사국(DEA)의 Digital Evidence Laboratory, 지

14) M. Pollitt, "Who is SWGDE and what is the history?", (http://68.156.151.124/SWGDE_History.pdf), 2003.
15) C. Whitcomb, "*An Historical Perspective of Digital Evidence: A Forensic Scientist's View*", International Journal of Digital Evidence, Spring 2002 1(1).
16) http://www.fbi.gov/pressrel/pressrel07/accretitation060707.htm 참조.

방 법집행기관으로는 Charleston 경찰국의 Digital Evidence Unit Laboratory 등이 최근 ASCLD/LAB 인증을 받았다.[17]

현재 미국에는 100개 이상의 대학에서 디지털 포렌식에 대한 학부와 대학원 과정을 개설되어,[18] 하나의 학문분야로 자리를 매김하고 있다. 한편 2006. 12월 미국은 연방 민사소송법(Federal Rules of Civil Procedure) 개정을 통해 디지털 포렌식 도구를 이용한 증거확보(e-discovery)를 의무화함으로써 이 분야 대한 성장세가 가속화될 전망이다.[19]

제4절 디지털 포렌식의 현대적 의의

로카르드(Edmund Rocard)가 최초의 포렌식랩을 프랑스 경찰에서 설치했던 것처럼 대부분의 법과학 분야의 시작은 감추어진 사실을 발견하기 위한 수사기관의 필요에 의해서 시작된다. 하지만 그것이 발달하기 시작하면 더 이상 특정한 목적을 지닌 수사기관의 요구에 전적으로 의지하지만은 않고 객관적이고 과학적인 원칙의 지배를 받는 독자적인 분야로 자리매김을 하기 마련이다.

오늘날 디지털 포렌식은 법과학의 한 분야로서 범죄수사와 민·형사상 재판에서 진실을 가리는 중요한 도구일 뿐 아니라 중요한 정보보안(Information Security)도구로, 또한 하나의 학문으로 혹은 하나의 산업으로 중요한 의미를 지니고 있다.

1. 법과학의 한 분야

법과학은 범죄수사를 돕는 도구일 뿐 아니라, 범죄수사의 맥락적(contextual)이고 목적 지향적인 경향에서 벗어나 그것이 과학적이고 객관적인 것이 될 수 있도록 균형을 잡아주는 통제장치이다. 법은 이러한 법과학이 좀 더 과학적이고 객관적인 될 수 있도록

17) http://www.ascld-lab.org/legacy/aslablegacylaboratories.html 참조.
18) http://www.usatoday.com/tech/news/techinnovations/2006-06-05-digital-forensics_x.htm 참조.
19) 임종인, 떠오르는 디지털 포렌식, 디지털 타임스 2006. 7. 18.자

하기 위해 속칭 쓰레기 법과학(junk forensics)이 법정에서 사용되지 않도록 하기 위한 규율을 제공하며 또 그렇게 하여야 한다. 이미 선진국에서 디지털 포렌식이 법과학의 한 분야로 뚜렷하게 자리매김을 해나가고 있음은 앞서 살펴본 바와 같다.

2. 정보보안 도구

디지털 포렌식의 특징 중의 하나는 폭넓은 적용가능성에 있다. 예컨데 살인사건의 현장에 대한 접근과 법과학의 적용은 극히 제한된 소수의 실무가와 부검의 등 전문가에게 제한되어 있다. 일반적인 공공기관과 기업들에 있어서 구내에서 살인사건이 일어날 것을 염려하여 미리 대비하는 것은 상상하기 어렵다. 하지만 정보보안과 관련된 침해의 위협은 오늘날 모든 공공기관, 기업, 개인에게 일상화된 문제이다.

이러한 위협이 실제로 사고로 이어졌을 때 그 사고를 인지하고 조사하기 위해 디지털 포렌식 기술은 크게 도움이 된다. 포렌식은 또한 그 사고의 원인이 무엇이었으며 누구에게 책임이 있는 지 분명히 해서 앞으로 그러한 일이 다시 일어나지 않도록 예방하고 누가 그 일에 책임이 있는지 가릴 수 있게 해준다.

이러한 정보보안 사고가 법적인 분쟁으로 이어질 개연성은 매우 높다. 이러한 법적인 분쟁은 사원들의 불법적인 행동이 회사에 손해를 끼치지 않을 것인지 감시하는 과정 혹은 그 결과에서도 발생할 수 있다. 따라서 사고를 조사할 때는 법적으로 향후 증거로써 사용될 수 있도록 포렌식의 원칙에 따라야 하는 이유이다. 국내외에서 많은 디지털 포렌식 관련 학과가 정보보안을 다루는 학과에 설치되어 있는 것도 그와 같은 맥락에서 파악될 수 있다.

미국의 E-discovery는 기업의 디지털 포렌식에 대한 관심이 정보보안이라고 하는 특수한 목적에서 벗어나 그 사용범위를 크게 확장할 필요성이 있음을 극명하게 보여준다. 향후 디지털 포렌식 기술은 기업경영에 있어 위험관리, 내부통제나 감사, 거래의 신뢰성 확보 등 여러 측면에서 중요한 기술이 될 것이다.

3. 하나의 학문분야

디지털 포렌식은 이제 법과학의 한 분야의 자리매김에서 벗어나 많은 선진국 대학에서 관련 학과를 설치하고 있는 하나의 학문 분야로서의 가능성을 보여주고 있다. 모든 법과학 분야가 이렇듯 대학에서 별도의 학과를 설치할 정도의 위치를 점하고 있는 것은 아니다.

학문으로서 디지털 포렌식은 대학에서의 더 많은 연구와 개발의 가능성을 보여주고 있다. 물론 대학에서의 디지털 포렌식, 특히 학위 과정이 개설되기 위해서 검토되어야 할 많은 점들은 아직 논란이 완전히 해소된 것이 아니다. 학문으로서 디지털 포렌식의 체계화가 어느 정도 진척된 것인지, 어떻게 커리큘럼을 구성할 것인지, 어떠한 자격이 있는 사람이 가르칠 것인지 등에 대한 많은 문제들이 있다.

반면 이러한 변화는 향후 디지털 포렌식의 전문성이 지금까지 단편적인 기술이나 제품 위주의 실기 능력만으로 완전히 자격을 인정받기 보다는 대학에서 정규적인 디지털 포렌식 교육을 받은 사람들에게 보다 쉽게 인정되는 추세를 보일 것이라는 예상을 가능하게 한다.

4. 첨단산업으로서의 디지털 포렌식

디지털 포렌식과 관련된 산업은 소프트웨어나 하드웨어와 같은 제품 뿐 아니라, 교육과 컨설팅, 일반 기업이나 로펌 등을 대상으로 한 상업화된 디지털 포렌식 서비스 등 매우 다양하다.

2002년 미국 컴퓨터 포렌식 시장은 1.33억 달러에서 2004년에는 2.84달러, 2009년에는 6.30 달러에 이를 것으로 전망되었으며 전 세계적으로는 18억 달러에 이를 것으로 추산되고 있다.[20]

디지털 포렌식 제품의 특징 중의 하나는 제품이 단순한 성능이 아니라 표준이나 검증과 같은 질적인 측면에서의 엄격한 평가를 받아야 한다는 점이다. 향후 이러한 점은 아직 디지털 포렌식 시장의 불모지나 다름없는 국내의 업체에서 제품을 개발한다고 하더라

20) Digital Forensics Curriculm Consortium (http://www.networksecuritytech.com/ITDF/pa.php 참조)

도 적절하게 시장으로 진입하는데 큰 장애가 될 우려가 크다.

현재도 대부분의 포렌식 제품은 미국 등 선진국의 제품을 수입하여 사용하고 있으며 그러한 제품을 적절하게 사용하기 위한 교육비 또한 많은 국부의 유출을 가져오고 있다. 이로 인해 국내 디지털 포렌식의 실무자들이 외산 제품에 점차 익숙해진다면 이 또한 향후 국내 디지털 포렌식 산업이 발전하는데 장애요소가 될 것이 분명하다.

다행히 일부 정부기관이 이러한 문제점들에 대한 인식 하에 국내 제품의 개발에 나서고 있는 것은 그러한 측면에서 바람직한 것으로 여겨진다.

제5절 디지털 포렌식의 일반적인 절차

대체적으로 범죄현장에서 수집된 증거가 포렌식랩에서 분석되어 결과물인 보고서가 작성되기까지의 전부 혹은 일부에 있어 절차적인 모델에 기반하여 디지털 포렌식 체계가 이루어지고 있다고 볼 수 있다. 디지털 포렌식 절차에 대한 절차 모델들은 이미 많은 학자와 전문가들에 의해 제시되고 있다.[21] 예컨데 미 법무부의 가이드라인[22]은 디지털 증거의 처리과정을 평가, 획득, 분석, 문서화와 보고의 단계로 구분하고 있다.

전형적으로 전반의 두 과정, 평가와 획득은 범죄현장에서 현장에 임장한 수사관에 의해 이루어지며 나중의 두 과정 조사와 문서화 및 보고는 증거가 포렌식랩으로 이송된 이후에 전문적인 포렌식 조사관 혹은 분석관에 의해 이루어진다. 이러한 일반적인 절차는 전통적인 물리적 증거의 처리 절차와 다를 바가 없다.[23]

수사절차의 단계 모델 자체에서 디지털 증거와 일반적인 물리적인 증거를 수사하는 과정을 구분하는 모델이 제시되기도 하였다. Carrier와 Spafford의 통합 디지털 수사 모델이 대표적인 형태로 <그림 1>과 같이 이를 도식화 한다[24].

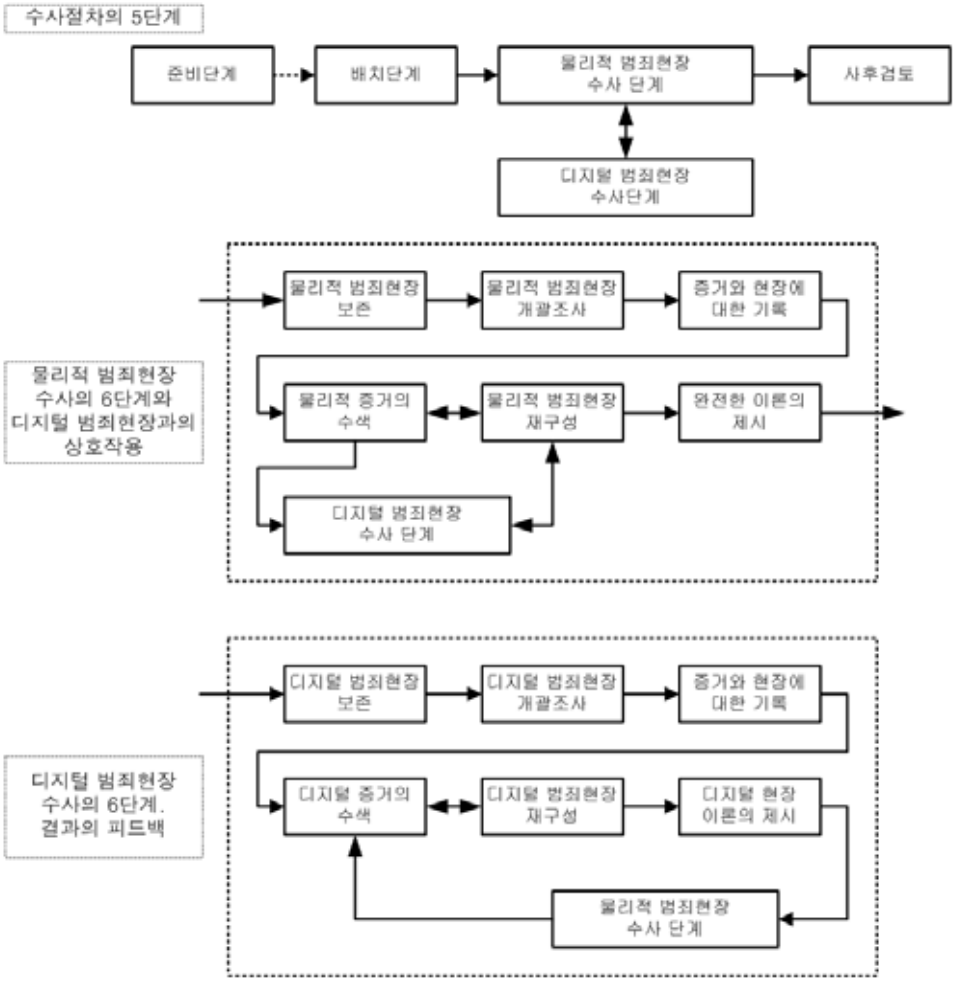
---

21) W Ren, *Ibid,* p.58.

22) U.S. Department of Justice, "*Forensic Examination of Digital Evidence: A Guide for Law Enforcement",* 2004.

23) 장윤식, "정보기술 아키텍처 기반의 디지털 포렌식 체계 도입에 대한 연구", 경찰학연구, 7(2): 65-84, 2007.

<그림 1> Carrier와 Spafford의 통합 디지털 수사 모델

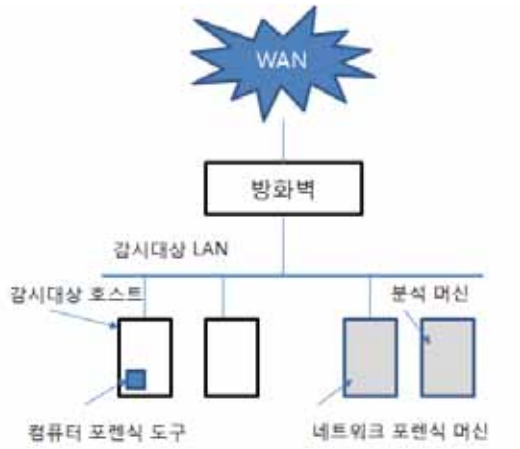


좀 더 넓은 의미에서 포렌식을 접근하는 시각들도 존재한다. <그림 2>와 <그림 3>은 인트라넷에서 실시간으로 전송되는 인터넷 패킷을 캡처하는 등 일명 스니핑(sniffing)을 이용한 네트워크 감시 형태의 증거수집 방법과 이를 포함하여 네트워크 기반의 포렌식에

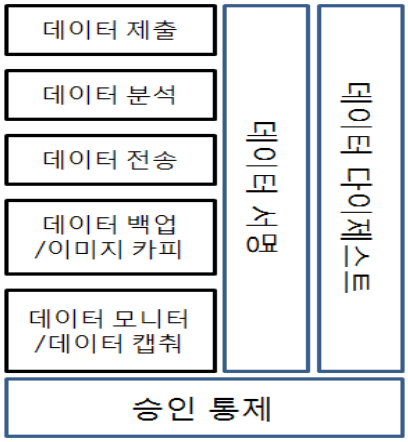
24) B. Carrier and E. Spafford, "*Getting Physical with the Digital Investigation Process*", International Journal of Digital Evidence, Fall 2003 2(2):7-10.

서의 아키텍처에 대한 모델을 보여주고 있다.[25] 이러한 포렌식 방법론은 사고대응(Incident Response)이나 범죄수사상 흔히 사용할 수 있는 방법들이지만 실시간으로 정보를 수집함으로 원본 증거를 어떤 것으로 볼 것인지, 따라서 어떻게 무결성을 검증할 수 있을 것인지 등에 대한 문제들이 제기될 수 있으며 앞선 모델들을 기반으로 한 수사 방법론으로 일부 설명이 곤란한 부분이 고려되고 있다는 점에서 진일보한 접근방식이라고 볼 수 있을 것이다. 하지만 아직 이러한 좀 더 넓은 범위의 연구는 미미한 실정이다.

<그림 2> 인트라넷에서의 네트워크 포렌식



<그림 3> 컴퓨터 네트워크 포렌식 시스템 아키텍처



제6절 범죄수사, 범죄현장, 법과학

디지털 포렌식을 포함해서 범죄수사와 법과학이 관여되는 핵심적인 지리적 공간은 범

25) W. Ren, Ibid, p.63. 저자는 논문에서 호스트 컴퓨터에 대한 포렌식 방법을 주로 의미하는 Computer Forensics에 덧붙여 네트워크 기반의 증거수집과 아키텍처 등 Computer Forensics를 확장하여 최광의의 의미로 Network Forensics라는 용어를 사용하고 있다.

죄현장(crime scene), 포렌식랩(forensic laboratory), 그리고 수사관의 사무실이다. 수사관의 사무실은 법적 권한을 가지고 범죄수사를 담당하는 수사관의 영역이다. 수사관의 1차적 목표는 범죄사건의 해결이다. 수사관은 수사기관에 속하며 때로는 사건해결을 촉구하는 수사기관의 상급자나 여론의 압력을 받으며 증거(evidence)와 단서(clue), 실마리(lead)를 둘러싸고 범죄자들과 힘겨운 싸움을 하는 사람들이다. 이들은 범죄자를 체포·신문하거나 영장을 신청하여 집행하는 법집행관(law enforcement officer)이다.

포렌식랩은 법과학 실무자(forensic practitioner)들의 영역이다. 국립과학수사연구소는 국내에서 독보적인 위치를 차지하고 있는 포렌식랩이다. 이들은 과학과 기술을 이용하여 증거를 검사하고 그 결과에 대한 해석이나 그들의 전문적인 지식에 기반한 자신들의 의견을 문서나 법정에서의 진술을 통해 검사를 의뢰한 사람들에게 제공한다. 검사를 의뢰하는 사람들은 법집행관일 수도 있고 법관일 수도 있다. 대부분의 국가기관에서 운영하는 포렌식랩에서는 피고인을 위한 검사의뢰를 받지 않는다. 이러한 의뢰는 사설 포렌식 서비스를 이용해야하는 경우가 많다. 하지만 여전히 포렌식 서비스는 공적인 서비스인 경우가 많으며 많은 경우 수사기관의 내부조직에 속해 있다. 공적기관을 위한 서비스를 제공한다는 대결적 구도의 한쪽에 놓여 있기는 하지만 법과학자들은 수사관과 같이 범죄해결 지향적, 조직의 요구보다는 과학의 원리와 염결성(integrity)에 의존하며 그 결과가 완전히 객관적인 것이 되도록 믿고 노력한다.[26] 이들의 신분 또한 국가나 조직별로 다양하다. 법집행관이 곧 법과학자 실무자의 역할을 수행하는 경우도 있고, 포렌식랩이 속한 기관에 소속은 되어 있지만 법집행관은 아닌 경우도 많다.

범죄현장(crime scene)은 포렌식과 관련된 업무의 대부분이 시작되는 곳이다. 위 절차 모델에서 본 것과 같이 많은 증거들이 범죄현장에서 수집되어 검사와 분석을 위해 포렌식랩으로 옮겨진다. 증거를 수집하는 사람은 법집행관이 될 수도 있고, 어떤 증거는 현장에서 식별(identification)하고 수집할 때부터 전문적인 지식과 기술이 필요하여 의뢰받는 법과학 실무자들이 수사관들과 함께 현장에 나가기도 한다. 사체에 대한 검시와 같은 고도의 전문지식에 의한 중요한 판단이 필요한 경우에 국가에 따라 보다 나은 형사사법 서비스를 위해서 법과학 실무자들에게 법집행관에게 없는 특별한 권한을 부여하기도

26) P. De Forest, R. Gaensslen, and H. Lee, Forensic Science: An Introduction to Criminalistics, McGrow-Hill, 1983, p.17.

한다. 법의관(medical examiner)과 검시관(coroner)제도와 같은 것이 그러한 것이다.

법과학자 전문가와는 구분되지만 일반적으로 범죄현장에서의 관찰과 증거수집은 특별히 훈련을 받은 사람들에 의해 수행되는 것을 믿어진다. 최근 CSI라는 미국 TV 드라마로 유명해진 범죄감식요원이나 현장조사관 혹은 수사요원(crime scene investigator)이라고 불리는 사람들이다. 현재 경찰에서 과학수사요원으로 호칭하고 있는 이들은 모두 현직 경찰관들이다. 하지만 비록 소속은 수사기관에 속해 있지만 법집행관이 아닌 전문적인 교육과 훈련을 받은 일반직(civilian)이 이 업무를 수행하는 나라도 많다. 특별한 지식과 기술을 요하는 디지털 범죄현장에서의 현장수사는 종래의 이러한 현장수사요원에 의해서는 적절하게 처리되기 어렵다.

위에서 언급된 업무와 이 업무를 담당하는 조직과 사람들을 어떻게 구성하느냐 하는 것이 법과학 서비스의 품질 나아가 범죄수사나 형사사법 서비스의 품질에 미치는 영향은 매우 크다. 하지만 법과학에서 이를 둘러싼 완전한 모범답안은 아직까지 발견되지 않았으며 따라서 각국의 시스템이 많거나 조금씩 다르게 유지되고 있다. 따라서 세부조직의 유무나 전문가가 현장에 나가는지, 어떤 역할을 하는 지의 여부와 관계없이 중요한 것은 수사관과 현장조사관, 그리고 포렌식랩 종사자간의 의사소통(communication)이라는 말[27]은 설득력이 있다. 그렇지만 법과학이 발달할수록 각 영역간에는 그 역할이 명확하게 구분되고, 임무를 수행하는데 있어서의 원칙과 그 일을 처리하는 사람과 부서의 자격요건이 엄격해진다.

제7절 법과학을 둘러싼 환경의 변화

법과학 서비스의 향상을 통한 형사사법 서비스의 개선을 바라는 시민들의 요구는 점차 거세지고 있다. CSI 효과(CSI effect) 혹은 신드롬(CSI syndrome)이라고까지 불리는 현상은 이러한 변화를 상징적으로 보여주는 것이다. 다소 현실과는 거리가 있는 TV 드라마를 통해 법과학에 대한 과도한 기대로 인해서 나타나는 제반 현상을 뜻하는 이 용어

27) P. Forest, R. Gaensslen, and H. Lee, *Ibid,* p.18.

는 실제로 법과학을 더 신뢰하거나 덜 신뢰하는 것과 같은 배심원에 대한 영향과 더 증거파괴에 신중을 기하게 하는 범죄자의 사고방식에 대한 영향 등이 연구된 바 있다. CSI Effect의 한 영향은 법과학 양성 프로그램에서도 나타난다. 최근 세계적으로 법과학과 관련된 대학학과에 등록하는 학생들의 수가 증가하는 현상을 보이고 있으며 이로 인해 대학들이 학생 수를 늘리기 위해 적절치 않은 학과 과정을 개설하여 전통적인 과학이론에 대한 철저한 학습 등 정규적인 코스를 거치지 않아 법과학 작업에 대비되어 있지 않은 졸업생들을 양산하여 법과학 서비스의 질을 저하시킨다는 수사기관의 비판도 있다.[28]

특히 국내에서 법과학은 매우 급격한 환경의 변화를 경험하고 있다. 공판중심주의와 국민의 사법참여를 골자로 하는 형사소송법이 개정되어 2008년부터 시행되면 배심제 하에서 증거법이 고도로 발달하게 된 영미법계에서 그랬던 것처럼 증거의 법적이 채택여부와 관련된 논란이 지금까지와는 비교할 수 없을 정도로 커질 가능성을 배제할 수 없다. 범죄현장에서의 수사는 이러한 문제들에 익숙한 법관이 아니라 전혀 사전지식이 없는 일반인을 설득하기 위해 훨씬 더 작업이 어려워질 가능성이 있다.

위법수집증거의 배제법칙을 개정 형사소송법에서 전격 명문화한 것은 증거수집에 관여하는 모든 사람들, 특히 수사관들이 증거수집에 지금보다 소극적인 태도를 보이게 하고 대신에 법과학에 좀 더 의존적인 태도를 보이게 할 가능성이 크다고 본다.

무역자유협정(FTA)에 따른 점차적인 법률시장개방이나 유비쿼터스로 대표되는 정보통신 서비스 환경의 변화 또한 모든 법과학 특히 디지털 포렌식에 큰 영향을 미치게 될 것으로 전망된다. 이러한 모든 변화들은 디지털 포렌식에 해결해야 할 수많은 과제를 던져줄 것이다.

---

28) Police Chief Criticizes Forensic Courses, (http://news.bbc.co.uk/1/hi/wales/3307089.stm), BBC News.

제3장 디지털 포렌식의 도전과제와 법과학 기반

디지털 포렌식은 다양한 측면에서 많은 논점들을 가지고 있다. 신흥 법과학의 한 분야로 종래의 법과학적인 요구사항을 충족하는 문제와 디지털 포렌식에만 고유한 원리와 원칙들을 반영하는 문제, 수사기관 등 소비자의 요구사항을 충족하는 문제, 법정에서 증거로 채택될 수 있도록 하기 위해 법적인 요구사항을 충족하는 문제와 같은 것들이 그것이다.

이러한 요구사항이 크게 법적인 측면, 기술적인 측면, 운영과 제도적인 측면에서 법과학계에 커다란 도전이 되고 있다. 그러한 문제들을 해결하기 위한 법과학계의 노력들은 일정한 체계를 형성하고 있다. 비단 그 세부적인 내용은 다르다고 해도 문제의 성격 자체는 디지털 포렌식에 한정된 것은 아니라고 할 것이다.

따라서 먼저 일반적으로 법적, 기술적, 운영 혹은 제도적 측면에서 디지털 포렌식의 과제들을 개괄적으로 살펴본 후 구체적으로 종래의 특정한 법과학 분야의 발전을 위한 노력이 주어지고 있는 법과학 기반의 구성요소들을 짚어 보겠다.

제1절 디지털 포렌식의 일반적 도전과제의 범주

1. 법적 도전(legal challenge)

가. 개 설

디지털 포렌식에서 다루는 법적 문제는 기본적으로 컴퓨터와 네트워크 등 정보를 처리하고 전송하는 장치와 그 대상인 정보, 즉 디지털 증거의 독특한 성격과 그것을 다루는 법과학으로서의 방법론에 대한 확고하지 않은 이론적 배경을 원인으로 한다. 법적 판단을 어렵게 하는 디지털 증거의 특징들은 이미 여러 연구에서 다루어져 왔는데 이에는 매

체독립성, 비가시성·비가독성, 원본과 사본 구별의 곤란성, 취약성, 대량성, 전문성, 네트워크 관련성과 같은 것이 포함된다.[29] 이러한 특성은 미국 National Center for Forensic Science(NCFS)에서처럼 디지털 증거를 종전의 물리적 증거나 생물학적 증거와 구분하거나[30] 증거법에 특별한 취급규정을 두는 것과 같이 디지털 증거를 별도의 증거로 다루도록 하고 있으나 다른 증거와는 전혀 별개의 독자적인 법상의 위치를 부여하는 것은 부분적으로는 가능하더라도 여전히 많은 경우는 기존의 준거틀 내에서 디지털 증거를 어떻게 해석할 것이냐에 관한 문제를 다루어야 한다.

위에서 "디지털 증거"라는 표현을 사용하였지만 디지털 포렌식에서 대상으로 하는 증거의 형태에 대해 1999년 SWGDE/IOCE의 Digital Evidence:Standards and Principles[31]에서는 다음 세가지를 들고 있다.

- ○ 데이터 객체(data objects): 물리적 항목과 연관된 잠재적 증거가치 있는 객체나 정보. 데이터 객체는 본래의 정보를 변경함이 없이 다른 형태들로 나타날 수 있다.
- ○ 디지털 증거(digital evidence): 디지털의 형태로 저장 혹은 전송되는 증거가치 있는 정보.
- ○ 물리적 물품(physical items): 데이터 객체나 정보가 저장되거나 그것을 통해 데이터 객체가 전송되는 물품.

이중 데이터 객체는 사실상 디지털 증거의 개념 안에 포섭될 수 있으며 대부분의 경우에 이를 구분하여 취급하지는 않는다. 따라서 디지털 포렌식에서 다루는 증거는 크게 디지털 증거(정보)와 물리적 장치(하드웨어)로 구분할 수 있다.

경찰에 있어 디지털 포렌식과 관련된 법적 논점은 형사절차법에 관한 것, 그 중에서도 증거법과 관련된 것들에 있다. 그 중에서도 가장 큰 문제가 되는 것은 디지털 포렌식과 관련된 증거의 수집절차에 관한 법적인 통제에 관한 부분과 수집된 증거의 법정에서의 증거능력의 인정여부에 관한 것이다. 전자에 대한 사전적인 통제는 수사기관 자체 내의

29) 양근원, 전게 논문, 22-26면.
30) http://www.ncfs.org 참조.
31) http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm 참조.

규율과 압수수색 영장 등 법적 허가의 부여 여부 등에 의해 이루어지며 사후적인 통제는 기본적으로 위법하게 수집된 증거의 증거능력을 법정에서 배제시킴으로써 이루어진다. 수집된 증거의 증거능력의 인정문제는 영미법에서 인용가능성(admissibility)의 문제로 이는 전자에 대한 법적 심사에 문제가 없음을 전제로 한다.

나. 증거획득의 적법성 문제

일반적으로 주된 관심사는 전자, 즉 증거의 수집 행위의 적법성의 문제라기보다는 법정에서 증거능력의 문제라고 볼 수 있다. 왜냐하면 증거 수집의 법적 권한을 획득하는 것은 디지털 포렌식 전문가보다는 일반적으로 수사권한이 있는 수사관의 문제이기 때문이다. 하지만 디지털 포렌식의 경우, 수집 대상 증거가 매체인지 혹은 그 안에 들어 있는 정보인지, 혹은 그 정보가 디스크에 저장된 파일과 고정(static)된 것인지 아니면 전송 중에 있는 정보처럼 유동적(dynamic)인 것인지, 그 정보를 보유하고 있는 주체가 누구인지, 공개된 것인지 등 여러 관점에서 법적으로 다양한 평가가 가능하다. 따라서 이를 규율하기 위한 법도 종래의 압수수색과 관련된 규정으로부터 다양한 정보의 형태별로 수집권한을 규율하기 위해 신설된 법에 이르기까지 여러가지를 고려해야 한다. 이러한 요구사항을 충족하는 방법 중의 일부는 다분히 기술적인 것이다. 예컨데 복잡하게 혼합되어 있는 정보 중에 법적으로 필요한 최소한의 정보만 추출하는 것은 간단한 문제가 아니기 때문이다.

다. 법정에서 증거능력의 인정 여부

법과학은 과학기술의 지식과 장비 등 도구의 도움으로 그것이 없었더라면 밝혀질 수 없었던 진실을 판단할 수 있는 많은 사실을 알려준다. 하지만 그 판단의 기초가 되었던 과학적 이론이 잘못된 것이라면, 검사 대상의 수집이나 검사과정에서 오류가 발생하였다면, 검사에 사용한 약물이 오염되거나 유효기간이 지나 의도한 바와 다른 검사결과를 나타냈다며, 누군가 증거를 고의나 실수로 잘못된 결과가 나오도록 오손하였다면 그 결과는 엉뚱한 사람을 범인으로 규정짓게 하거나 범인을 무고한 것으로 잘못 판단하도록 하는 심각한 결과를 낳게 된다. 아쉽게도 역사상 이러한 과학기술의 잘못된 적용으로 인한

법정에서의 잘못된 판결의 사례는 무수하게 많다.

게다가 많은 법과학적 지식을 적용하는데 있어서 사용되는 지식과 기술, 도구 등에 대한 과학과 기술의 지식이 옳은 것인지 많은 경우 분명하지 않다. 예컨데 최신의 DNA 검사방법과 그 검사결과의 해석방법에 대해서는 큰 논란이 없으며 법정에서 흔히 받아들여지고 있다. 하지만 사회·심리학적 분석, 프로파일링, 거짓말탐지기(polygraph) 검사결과 같은 분야 등은 법정에서 증거로 받아들여지지 않거나 여전히 논란의 대상이 되고 있다. 어떠한 분야는 쓰레기 법과학(junk forensics)로 여겨진다. 이러한 논란으로 인해 많은 검사결과는 법과학적 검사를 시행하고 보고서를 작성하거나 법정에서 증언한 사람에 따라 달라질 수 있기 때문에 그 사람의 자격이나 능력이 법정에서 논란이 된다. 디지털 포렌식 또한 이러한 논란의 가운데에 있다고 할 수 있다. 이른바 법과학 서비스의 품질의 보증(Quality Assurance)의 문제가 디지털 포렌식에서 심각하게 대두되는 것이다.

2. 기술적 도전(technical challenge)

컴퓨터와 네트워크라고 하는 고도로 발달하고 있는 기술적인 분야에 있어 수사기관에 기술적인 도전이 존재함은 너무도 명백하다. 앞에서 언급한 법적인 요구사항을 충족하면서 수사기관 등 디지털 포렌식의 소비자가 요구하는 서비스를 제공하기 위해 필요한 기술은 매우 방대한 영역에 걸쳐 있다.

고정되어 있거나 유동적인 정보를 그 출처로부터 추출하기 위해서는 특별한 장비와 소프트웨어 등 도구(tools)이 필요한 경우가 많다. 이러한 장비는 법적인 요구조건을 충족하기 위해 충분히 검증되어야 한다. 나날이 그 용량이 증가하고 있는 매체에서 발견된 대량의 데이터는 사람의 눈으로 직관적으로 알 수 있는 경우보다는 다시 특별한 도구와 고도화된 데이터 처리기술에 의해서 비로소 그 의미를 분명히 알 수 있다. 정보는 흔히 범죄자에 의해서 일반적으로 알아낼 수 없도록 암호화되거나 숨겨지며 파괴된다.

포렌식에 사용되는 장비와 도구들은 매우 다양하여 그것의 사용법을 익히고 이를 통해서 실제 증거를 수집하고 분석하는 포렌식 업무를 수행하는 것은 컴퓨터와 네트워크에 대한 점차 깊은 수준의 지식과 기술, 능력을 필요로 하고 있다.

3. 제도·운영상의 문제에의 도전(operational challenge)

법적인 문제와 기술적인 문제가 어떤 형태로든 정의될 수 있는 문제라면 제도와 운영상의 문제는 현실과 동적으로 관련이 되는 매우 복잡한 문제이다.

디지털 포렌식 업무의 수요는 얼마나 될 것인가에 따라 조직의 인력과 규모가 결정될 것이며 이들을 어떻게 교육훈련 시킬 것인지가 고려되어야 한다. 이 업무를 수사관이 병행하게 할 것인지 아니면 별도로 전담인력을 두도록 할 것인지, 그들에게 어떠한 장비과 도구를 제공할 것인지 그렇다면 예산은 어떻게 확보할 것인지와 같은 문제 또한 이 범주에 속하게 된다. 실제 조직과 인력이 있다고 하더라도 법에서 요구되는 법과학의 원칙을 어떻게 준수하게 하도록 할 것이며, 그것을 보증할 수 있는 방법은 무엇인가 또한 같은 범주에 속한 문제이다.

이러한 문제들과 관련된 제반의 사항들이 다름 아닌 디지털 포렌식의 기반 내지 체계에 관한 문제라고 할 것이다. 다행히 이러한 과제에 대한 선진국 법과학계의 대처는 오랫동안 이루어져 왔으며 많은 논란에도 불구하고 법과학의 제반 구성요소는 일정한 형태성을 띄고 있다. 하지만 아쉽게도 디지털 포렌식 뿐 아니라 전통적인 법과학의 기반이 아직 탄탄하지 않기 때문에 일부의 문제들은 대부분의 국내 수사기관이나 관련 산업계나 학계에서 아직 생소한 문제이기도 하고 이에 공동으로 대처하는데 어려움을 겪고 있다.

제2절 법과학 기반의 핵심 요소

법과학 서비스의 양과 질적인 수요를 감당할 수 있는 기반요소는 매우 다양한 하부요소들로 이루어져 있다. 여기에서는 전통적인 법과학에서 필요충분한 서비스를 제공하기 위해 갖추어야 할 기본적인 사항들을 통합세출법(The 2004 Consolidated Appropriations Act, H.R. 2673)에 의해 미 의회가 국립사법연구소(the National Institute of Justice)에 작성하여 제출할 것을 요구한 법과학 서비스 제공자들이 필요로 하는 수요조사의 결과[32]를 중심으로 살펴보겠다.

---

32) 이 보고서(*Status and Needs of Forensic Science Service Providers: A Report to Congress,*

1. 조직과 인력, 장비

충분한 수의 인력과 특화된 장비는 모든 법과학 분야에서 최고의 법과학 서비스 제공을 위한 필수요건이다. 법과학 서비스 요청이 제공 역량을 초과하면 의뢰 잔량(backlogs)이 발생하여 재판과 범죄수사에 심각한 지연을 초래하게 된다. 이 문제를 해결하기 위해서 법과학 연구실 등은 법정 기일 등에 따라 분석의 우선순위를 부여하거나 아무 용의자도 특정되지 않은 사건의 접수를 제한하는 정책을 수립하고 있으며 외국의 경우 극단적인 경우 의뢰된 증거물을 반송하는 사태까지 일어나고 있다. 이 문제를 해결하기 위한 가장 확실한 해결책은 부족한 인력을 보강하는 것이지만 대부분의 법과학 분야에서 인력의 부족 문제는 세계적인 현상이다.

미 사법통계국(the Bureau of Justice Statistics)의 조사[33]에 따르면 2002년도에 미국의 50대 범죄 연구실에서 접수한 사건 수는 994,000건, 의뢰된 증거물 수는 120만 건에 이른다. 2002년 중에 115,000건의 전년도에 이월된 미분석 잔량[34]에 120만 건을 새로이 의뢰받아 270,000건의 새로운 미분석 잔량을 남겨 놓았다. 이 50대 범죄 연구실은 4,300명의 전일제 인력을 보유하고 있으나 930명의 추가 인력이 필요한 것으로 파악되었다.[35] 이를 위해 3,600만 달러의 예산이 추가적으로 필요할 것으로 추산되었다. 또한 1,800만 달러 상당의 새로운 장비를 포함하여 실험실 공간, 시간 외 근무 수당, 출장비 등 추가 예산이 필요한 것으로 파악되었다.

국제감식협회(IAI) 조사에 따르면 66퍼센트의 지문감식은 전통적인 범죄 연구실이 아

NIJ, March 2006, NCJ 213420.)의 작성에는 미 국립사법연구소를 중심으로 전미 범죄 연구실 책임자협회(the American Society of Crime Lab Directors, 이하 ASCLD), 전미 법과학회(the American Academy of Forensic Science, 이하 AAFS), 국제감식협회(the International Association for Identification, 이하 IAI), 국립 법의관협회(the National Association of Medical Examiners, 이하 NAME)가 참여하였다.(http://www.ncjrs.gov/pdffiles1/nij/213420.pdf)

33) Bureau of Justice Statistics(BJS), *50 Largest Crime Labs 2002*, 2002

34) 인용한 보고서에서 미분석 잔량은 30일 이상 분석되지 않은 채로 남아 있는 증거물을 의미한다.

35) 이와 비교하여 같은 2002년 국립과학수사연구소는 180여명의 감정인력으로 175,277건의 감정의뢰물을 처리했으니(한면수 외, 과학수사론, 경찰대학, 2005) 미국보다 산술적으로 3~4배의 업무량을 소화하고 있음을 알 수 있다.

니라 경찰 혹은 보안관 사무실이나 주의 범죄국에서 이루어진다. 통상 이러한 곳에서 지문감식은 범죄현장계(Crime Scene Unit), 감식과 혹은 계(Identification Division or Unit), 지문계(Fingerprint Unit)에서 이루어진다. 이러한 곳에서 많은 지문분석가는 법집행관(sworn law enforcement officer)들이며 좀 더 많은 인력과 컴퓨터 장비, 훈련이 필요하다. 이러한 실정은 디지털 포렌식의 경우에도 마찬가지이다.

필요한 인력의 판단은 단순히 의뢰량에 의존해서 판단할 수 없다. 후술하겠거니와 디지털 증거에 대한 인식은 많은 수사기관에 아직 확고하지 않다. 즉, 필요한만큼 충분히 증거를 수집하여 검사가 되지 않고 있다는 것이다. 게다가 미국의 경우 디지털 법과학 분야에서도 또한 보다 많은 인력이 필요하지만 상대적으로 적은 근무시간과 많은 보수에 이끌려 고급 수사관들이 민간 분야로 옮겨가 인력 부족이 심화되고 있다.

2. 지속적인 교육

법과학계에서는 훈련 수요가 매우 심각하며 분야별로 다양하다. 신규와 유경험자에 대한 보수교육을 통해 범죄 연구실은 사법시스템에 최고의 서비스를 제공할 수 있다. 증거를 분석하기 위해 법과학 분석가들은 기초적인 과학 교육과 영역별로 특화된 훈련을 필요로 한다. 널리 받아들여지고 있는 인증 표준에 부합하기 위해 최소한 자연과학, 법과학 혹은 이와 밀접한 분야에 대한 학사 학위를 필요로 한다.[36] 교육과 훈련은 또한 전문성을 유지하고 지식과 기술을 업데이트하며 발전과 변화를 따라가기 위해 필수적이다. 새로운 분석가나 검사관이 고용되었을 때 자격을 갖추기 위한 초기 훈련을 필요로 한다. 훈련기간은 영역에 따라 다른데, 통제 물질 분석가의 경우 6~12개월의 훈련을 필요로 한다. 경험기반의 영역인 잠재지문 분석, 화기 및 공구흔, 문서감정의 경우 독자적으로 분석 업무를 하기에 앞서 3년 이상의 훈련을 필요로 한다. 보수교육에 대한 요구사항 또한 영역별로 다양하다.

36) 후술하는 ASCLD/LAB 등의 인증을 의미한다. 유사한 인증의 대부분은 법과학 분야의 검사관들에게 과학 분야에 대한 학사 학위를 요구한다.

이러한 교육과 훈련의 내용이 어떠한 것이 되어야하며 디지털 포렌식 검사관에게 어떠한 수준의 능력이 있어야 하는지에 대한 판단은 실제 교육과 훈련에 앞서 엄밀하게 판단되어야 한다.

가. 법과학 교육

최근 대학가에서 많은 수의 법과학 교육[37] 프로그램이 신설되었다고 하지만 법과학 교육 심의회(the Council on Forensic Science Education, COFSE)는 많은 법과학 교육 프로그램이 매우 제한적인 자원과 불충분한 인력, 실험실 공간 그리고 지원을 가지고 있다고 밝혔다.

1999년 국립사법연구소(NIJ)는 '법과학: 현재상태와 수요 검토'라는 법과학에 대한 평가를 통해서 법과학 분야에 대한 교육 및 훈련 수요가 매우 심각하다며 다음과 같은 사항에 대한 권고를 하였다.

- 법과학 교육에 대한 국가적 표준
- 독립적이고, 법과학계 전체를 반영하며, 공감대를 형성하고, 표준을 설정할 수 있는 법과학 교육에 대한 기술 워킹그룹
- 법과학 교육 프로그램에 대한 인증(accreditation) 시스템

2001년 국립사법연구소는 법과학 교육과 훈련을 위한 기술 워킹그룹(Technical Working Group for Education and Training in Forensic Science)를 설치하였고 TWGED 2003년 '법과학의 교육과 훈련: 포렌식랩, 교육기관, 학생들을 위한 가이드'[38] 라는 연구보고서를 발간하였다. 전미 법과학회(the American Academy of Forensic Science, AAFS)는 국립사법연구소(NIJ)의 지원을 받는 Technical Working Group on Education and Training in Forensic Science(TWGED)의 가이드라인에 포함

37) 통상 교육(education)이란 대학에서의 교육을 의미하며 직업적이고 특수한 목적에 특화된 훈련(training)과 구별되는 의미로 사용된다.

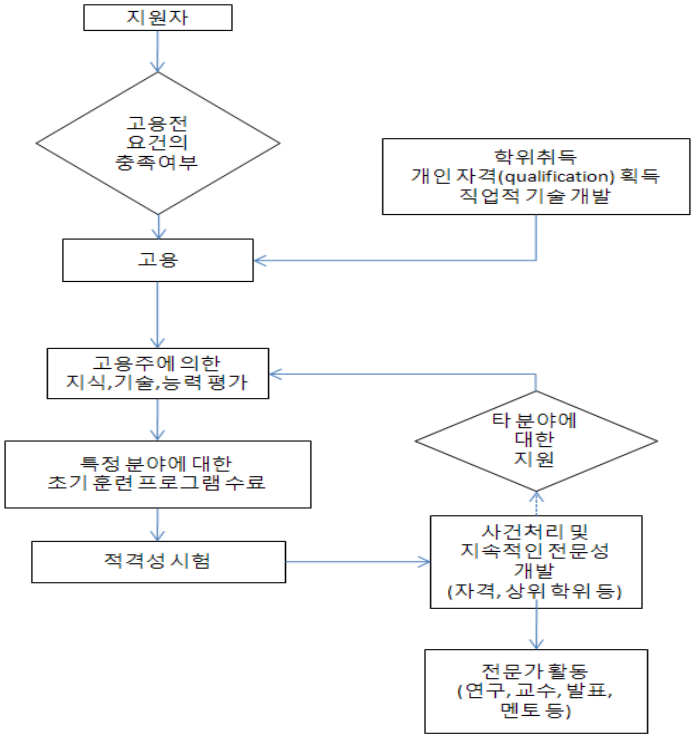
38) NIJ, "*Education and Training in Forensic Science: A Guide for Forensic Science Laboratories, Educational Institutions, and Students*"(http://www.aafs.org/pdf/NIJReport.pdf), June 2004.

된 대학 수준의 학술 프로그램에 대한 공식적인 평가와 인정을 위한 프로그램을 만들기 위해 법과학 교육 프로그램 인증 위원회(the Forensic Educational Programs Accreditation Commission, FEPAC)를 설치했다. FEPAC은 2004년 대학의 법과학 프로그램 인증을 위한 표준, 정책, 절차를 마련해 인증업무를 시작했다. 이 프로그램은 인증을 받기 위한 대학의 자기 학습과 훈련된 FEPAC의 평가자에 의한 현장 평가를 포함한다.[39]

위 TWGED의 가이드라인에서는 <그림 4>와 같이 법과학 분야의 경력개발 모델을 제시하고 있다. 고용전 요건으로 모든 지원자는 개인적 염결성과 자연과학에 대한 학사학위(최소), 또한 다른 권고사항을 충족하기 위한 추가적인 지식, 기술, 능력(Knowledge, Skill, Ability)를 지니고 있어야 할 것으로 제시했다.

구체적으로 먼저 법과학 종사자가 형사사법 시스템에 속하기 때문에 개인의 정직성, 염결성(integrity), 과학적 객관성 등 개인 특성(personal characteristics)이 매우 중요하다고 하고, 법집행관과 유사한 배경조사(backgound check)가 필요하며 마약검사, 마약투약전력, 범죄경력, 주변관계, 거짓말탐지기 검사, 운전기록, 과거 직업에서의 업무수행, 신용상태, 의학적 신체적 검사 등이 고용전에 검사되어야 한다. 대학교육(academic qualification)에 대해서는 분야별로 요구되는 학위수준이 다른데 위 가이드라인의 출간 당시에 신규 분야인 디지털 포렌식 분야에 대해서는 추가적인 검토가 있을 것이라고 했다. 또 다른 중요한 요소인 직업적 능력(professional skill)에 대해 비판적 사고(정량적 추리와 문제해결), 의사결정, 좋은 랩 실기, 랩 안전에 대한 경각심, 세부적인 사항에 대한 관찰과 주의, 컴퓨터 사용, 대인 관계 기술, 공적인 말하기, 구두와 문서화된 커뮤니케이션, 시간관리, 업무의 우선순위 결정

39) AAFS Forensic Science Education Programs Accredatation Commission, "*Accreditation Standards*"(http://www.aafs.org/pdf/FEPAC%20Accreditation%20Standards%20_082307_.pdf), August 23, 2007.



<그림 4> 법과학 분야의 경력개발 모델

TWGED 가이드라인은 법과학 프로그램에 대한 재정지원을 권고하고 있다. 법과학 분야에서 대학원 교육은 사법의 다른 분야에서와 달리 전용의 사법 재정지원을 받지 못하고 있다. FEPAC의 인증 표준에 따른 요구사항에 따른 석사 학위를 따기 위한 연구 비용은 한 학생당 평균 만 오천에서 이 만 달러에 이른다.

연구실 인증 표준은 훈련이 문서화되어야 하며 자격을 나타낼 수 있는 것이 되어야 할 것을 요구한다. 한 명의 분석가에 대한 1년간 교육 프로그램 인건비 지출은 3만에서 4만 달러에 이르지만 생산성 향상으로 상당 부분 보충될 수 있다고 믿는다. 법과학 실무자의 초기 훈련 부담을 줄이기 위한 방문과학자나 인턴 프로그램 또한 부분적으로 존재하지만 비용이 높은 대신에 재정지원은 매우 적은 편이다.

나. 전문 보수 교육

전문 보수 교육은 대부분의 과학 기술 실무그룹과 자격, 인증 프로그램에서 요구되지만 분야별로 내용과 기간은 상이하다. 이에 대한 외부의 재정지원 프로그램은 아직 없다. 예를 들어 FBI의 법과학 DNA 검사 연구실 품질보증 표준(The FBI's Quality Assurance Standards for Forensic DNA Testing Laboratories)은 매년 최소 8시간의 보수 교육을 요구하며 범죄 연구실 대표협회/연구실 인증위원회 인증 프로그램 또한 이 조건을 받아들여 모든 DNA 분석가들에게 같은 요구를 하고 있다. TWGED는 전체 법과학 연구실 예산의 1 내지 3 퍼센트를 훈련과 지속적인 전문성 개발에 할당할 것을 권고하였다. 하지만 사법통계국의 조사에 따르면 50대 연구실에서 실제로는 0.5 퍼센트 이하의 예산만이 사용되고 있었다.

감독자나 책임자들 과학분야에 대해 교육을 받기도 하지만 법과학계에서는 기초 경영과 인사관리, 회계 절차, 프로젝트 관리에 관한 교육이 필요하다고 본다. FBI와 ASCLD는 참석자의 참가 비용을 부담하고 연례 연구실 운영에 관한 심포지엄을 개최하기도 한다. 웹기반의 FBI 가상 학교, 일리노이 주 경찰 등의 비디오 컨퍼런스 같은 새로운 훈련 시스템 또한 고비용의 교육, 훈련에 대한 대안으로 증가하고 있다.

디지털 증거 분석 분야는 빠르게 변화하는 분야 중의 하나이다. 이 분야에 대한 인증체계는 ASCLD/LAB에 채택되었지만 디지털 법과학 실무자에 대한 국가적인 표준 혹은 자격심사 제도는 아직 존재하지 않는다.

3. 전문성과 인증표준

법과학계에서 전문성을 유지하고 향상시키는 것은 많은 이슈를 포함하는 문제이다. 전문성은 실험실 인증과 검사관·분석가 자격공인, 전문가 조직의 가이드라인과 같은 것들에 의해 유지된다. 연구, 혁신, 기술이전과 같은 것 또한 전문성을 이루는 요소들이 된다.

가. 범죄 연구실 인증

포렌식랩의 인증(accreditation)[40]은 실험실이 품질 관리를 위한 문서화된 정책을 유지하고 준수할 것을 요구한다. 인증은 제품, 공정 또는 서비스가 규정된 요건을 충족시키는 정도에 대한 체계적인 심사를 뜻하는 적합성 평가(conformity assessment)의 방법으로, ISO/IEC guide 2에 따르면 인증(accreditation)이란 특정한 작업의 절차를 수행할 능력을 가진 피인증 기관에 대한 상위 기관의 승인을 뜻한다.

포렌식랩에 대한 인증은 널리 알려진 ISO/IEC[41] 국제인증과 각 국가 또는 기관의 개별적인 인증이 있다. ISO/IEC 인증에 있어 포렌식랩은 법과학과 관련없는 일반적인 다른 실험실과 함께 교정·시험기관(calibration & testing laboratory) 인증을 받고 있다. 국내에서 교정·시험기관에 대한 인증업무는 산업자원부 기술표준원 산하 한국교정시험기관 인정기구(KOLAS)에서 수행하고 있다. 이 인증에 사용되는 국제기준은 ISO/IEC 17025이며 이를 한글화한 기준은 기술표준원 고시인 KS A ISO/IEC 17025이다.[42] 한편 KOLAS는 법과학시험기관의 인증업무에 관하여 KOLAS 지침(KOLAS G-006:2007, 기술표준원 고시 제2007-138호)을 2007년 4월부터 정하여 운영하고 있다. 하지만 ISO 인증은 디지털 포렌식랩은 물론 일반적인 포렌식랩 뿐 아니라 모든 교정·시험기관의 인증에 활용되기 때문에 법과학적인 특수성을 완전히 반영하기 곤란한 측면이 있다.[43]

---

40) Accreditation, 제품이나 품질시스템의 경우 ISO/IEC guide 61에 따른 인정기구가 정부로부터 지정되면 해당 인정기구가 실제 제품과 품질시스템을 인증(certification)하는 기관을 심사(인정)하여 그 인증기관이 실제의 인증을 하는 체계에 따르나, ISO/IEC guide 58에 따른 교정시험기관의 경우 정부로부터 지정받은 인정기구(국내의 경우 기술표준원 산하 한국교정시험기관인정기구)가 각 교정시험기관에 대해 바로 인정을 하며 용어 또한 인정이라고 하고 있으나 본고에서는 널리 사용되는 용례, 특히 최종적인 적합성심사를 뜻하는 의미에서 accreditation을 인증이라고 표현하기로 한다.

41) International Organization for Standardization/International Electrotechnical Commission

42) 2007년 11월 현재 이 인증을 받은 국내 법과학시험기관은 규제 물질류 검사, DNA형 검사 등 5개 영역에 대한 인증을 받은 국립과학수사연구소와 3개 영역에 대한 인증을 받은 대검찰청이 있을 뿐이다.

43) M. Simon and J. Slay, "*Forensic Computing Training, Certification and Accreditation: An Australian Overview*", in IFIP International Federation for Information Processing, 237, Fifth World Conference on Information Security Education, eds. Futcher, L., Dodge, R., (Boston: Springer), pp. 105 - 112.

지역적으로 특화된 포렌식랩에 대한 인증으로 가장 명성이 높은 인증은 미국 법과학시험기관장협회 시험기관인증위원회(American Society of Crime Laboratory Directors/Laborotary Accreditation Board, ASCLD/LAB)프로그램이다.

이 프로그램은 현재 국제표준기구(ISO)의 표준에 부합하는 국제표준 프로그램을 포함하고 있다.[44] 따라서 ASCLD/LAB 인증과 ISO 인증은 많은 부분에서 요건을 공유하고 있다고 볼 수 있는데 ASCLD/LAB 인증이 좀 더 포렌식랩에 특화되고 요건이 까다롭다고 할 수 있다. 한편 이러한 인증의 요구사항은 일반적인 방향성만을 정해주는 것이지, 세부적·구체적으로 그 요건에 맞는 시스템의 구축은 여전히 포렌식랩 운영자의 몫이라는 점을 인식하여야 한다. 예를 들어 디지털 증거의 특성에 맞는 증거물의 관리요령에 대한 명확한 지침을 ASCLD/LAB 인증 요건에서는 제시되지 않는다.

ASCLD/LAB 인증에서 요구되는 사항은 랩의 경영과 운영 차원에서 랩의 목적, 행정적인 책략, 권한의 부여, 관리감독, 구성원간의 커뮤니케이션, 훈련과 개발, 증거와 개별특성 데이터베이스 표본의 관리, 품질시스템의 운영 등이 고려된다. 개인에 대해서는 통제물질, 독물학, 디지털과 멀티미디어 증거 등 10개 분야 각각에 대해 적격성 기준을 제시하고 있다. 또한 포렌식랩의 공간, 설계, 보안, 건강과 안전 등 물리적 설비에 대한 기준 또한 포함하고 있는 등 포렌식랩의 적격성을 판단하기 위한 매우 방대한 양의 자격기준을 제시하고 있다. 따라서 사실상 포렌식랩의 인증제도는 포렌식 서비스의 질을 향상시키기 위한 여러 제도들을 모두 포괄하는 집합체라고 해도 과언이 아니다.

한편으로 이러한 인증은 주로 전통적인 의미의 범죄 연구실에서 이루어지는 것으로 여겨지나 실제 법과학 서비스의 다수는 이러한 전통적인 범죄 연구실이 아닌 과학적인 훈련을 받지 않은 법집행관이 포함된 기관에서 이루어진다는 것을 유념해야 한다. 범죄 연구실의 개념을 14,000의 경찰 기관과 다른 법집행 기관의 감식부서에 까지 확장한다면 미국에는 1,000개 가량의 법과학 서비스 제공기관이 존재하지만 정확한 숫자는 알 수 없다. 평균적인 전통적 법과학 연구실의 인력은 30명(이중 분석인력은 25명)이며 (경찰

44) 2007년 2월 현재 ASCLD/LAB 인증을 받은 범죄 연구실은 전체 330개로, 22개 연방 연구실, 180개 주 연구실, 100개의 지역 연구실, 10개의 해외 연구실을 포함한다. 인증을 받은 해외 연구실은 싱가폴, 캐나다, 말레이시아, 홍콩, 뉴질랜드 등에 소재한 것들이다(http://www.ascld-lab.org 참조).

서 등에 설치된) 비전통적 법과학 연구실 인력 평균은 3명이다. 인증을 통한 품질보증 표준에 부합하는 범죄 연구실 확보에 대한 중요성이 강조되고 있지만 예산 등 지원이 이를 따라가지 못하고 있다.[45]

나. 개인자격 공인

실무자들이 특정한 표준에 부합하는가를 판가름하기 위한 많은 수의 자격공인 위원회가 있다. AAFS를 통해 결성된 법과학 전문성 인증 위원회(The Forensic Specialties Accreditation Board)는 이러한 인증 프로그램을 평가하고 공인하고 감시하기 위한 표준과 프로그램을 개발해왔다. 이러한 절차는 ISO 국제 표준에 기반하고 있다.

45) Status and Needs of Forensic Science Service Providers: A Report to Congress, *Ibid.*

제4장 미국의 디지털 포렌식 발전 현황

앞서 디지털 포렌식의 역사에서 살펴본 바와 같이 주요한 많은 디지털 포렌식의 발전은 미국을 중심으로 이루어졌다고 해도 과언은 아니다. 이것은 아무래도 정보통신 관련 기술의 주요한 발달이 미국에서 이루졌기 때문이기도 하겠지만 디지털 포렌식의 수요를 창출하는 많은 사이버 관련 범죄, 이와 덧붙여 기존에 법과학에 관한 여러 가지 문제점들에 대한 인식과 이에 대응하기 위한 공감대의 형성과 방법에 대한 익숙함이 큰 영향을 주었을 것으로 생각된다.

제1절 미국의 디지털 포렌식 수요

미국은 대략 18,000여개에 이르는 연방, 주, 지방의 법집행기관이 존재하며 각 기관의 구성이나 역할이 제각각이기 때문에 법집행 분야에서 전국적인 통계를 산출하는 것이 쉬운 작업이 아니며 간접적인 방법으로 이를 예측해볼 수 있을 뿐이다.

컴퓨터와 관련된 범죄에 대응해야 하는 법집행기관들은 훈련이나 장비, 인력 등의 부족과 심각성에 대한 인식부족 등의 문제점을 노출하여 왔는데 특히 국립사법연구소의 한 보고서에서는 공공의 인식, 데이터의 보고, 정규화된 훈련과 자격제도, 전자범죄에 대한 관리적 지원, 법률정비, 산업계와의 협력, 특별한 연구와 출판, 관리적 인식과 지원, 수사와 포렌식 도구, 컴퓨터 범죄 부서의 설치 등의 10대 문제점이 제시된 바 있다.[46]

RCFL은 포렌식 서비스 요청을 의뢰받은 사건들을 테러리즘, 대간첩, 사이버범죄, 공공부패, 시민권침해, 조직범죄, 화이트칼라범죄, 주요절도/폭력범죄 등으로 8종으로 분류하고 있다. 이중 13개 RCFL 중에서 11개의 RCFL에서 가장 많은 서비스 요청이 들어온 사건의 형태는 사이버범죄이다. 사이버공간에서 벌어지는 사이버범죄의 특성상 당연히 디지털 증거의 비중이 타 범죄 비해서 많을 것이며 사이버범죄를 수사하는 기관에서

46) H. Stambaugh, et. al., "*State and local law enforcement needs to combat electronic crime",* National Institute of Justice Research in Brief, 2001.

디지털 증거에 대한 체계적인 검사에 대해 더 많은 지식이 있기 때문에 더 자주 의뢰를 하리라는 분석이 가능하다.

하지만 미국에서 실제로 얼마나 많은 사이버범죄가 발생하고 있는지는 알기 어려운데, 이는 무엇보다 법집행기관에 인지된 전국적 범죄통계인 UCR(Uniform Crime Report)에서 아직 사이버범죄에 대한 별도의 통계를 작성하지 않기 때문이다. 대신 FBI가 National White Collar Crime Centre(NW3C)와 함께 운영하는 Internet Crime Complaint Center(IC3)를 통해 접수받는 인터넷 관련 범죄의 추세를 통해 개략적인 범죄현황을 살펴볼 수 있는데, 2006년의 경우 207,492건의 신고를 받아서 200,481건이 처리되었는데 이 중에는 86,000건 가량이 실제 수사 등을 위해 각급 법집행기관에 이첩되었고, 114,000건은 추세분석에 사용되었다. 이러한 범죄에는 온라인 사기, 지적재산권 침해, 해킹, 산업기밀 유출, 아동포르노, 개인정보 침해와 돈세탁 등이 포함된다[47]. 이는 2000년 이래 2005년 231,493건까지 계속 증가하다가 2005년 대비 10.4%가 감소한 수치[48]이다. 한국 경찰에서도 이와 유사한 통계를 산출하고 있기 때문에 간접적으로 양자에 대한 비교가 가능할 것이다.

디지털 증거에 대한 법집행기관의 인식에 대한 최근의 조사[49]에 따르면 훈련받은 수사관의 부족과 다량의 전자적 증거에 문제에 대처하기 위한 가용가능한 절차의 부족, 디지털 포렌식 분야에서의 표준의 부재와 실무자에 대한 자격의 결여와 같은 문제가 지적되었다. 대부분의 전문가들은 디지털 포렌식이 과학적, 법적으로 DNA나 잠재지문 분석과 같은 상태에 이르려면 체계적인 교육과 연구, 개발이 필요하다고 지적하고 있다. 법집행기관은 디지털 증거를 추출하고 분석하는 좀 더 고도화된 도구, 특히 광범위한 분석 네트워크 환경에 있는 증거에 대한 대응이 필요하다고 인식하고 있다. 또한 장비와 인력, 교육과 훈련에 대한 수요가 인지되고 있다.

---

47) S. Hilley, *US cybercrime statistics: FBI hotline gets more than 200,000 complaints,* Digital Investigation, 4(2007) 54-55.

48) Internet Crime Complaint Center, *2006 Internet Crime Report*, (http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf), 2007.

49) M. Rogers, et al., *"Survey of Law Enforcement Perceprtion Regarding Digital Evidence"*, 2007, in IFIP International Federation for Information Processing, Volume 242, Advances in Digital Forensics Ⅲ; eds. P.Craiger and S Shenoi;(Boston: Springer), pp. 41-52.

FBI는 대략 80% 이상의 범죄사건에서 디지털 증거를 포함하고 있으며 사건당 디지털 증거의 분량이 증가하고 있다. 반면 주와 지방 법집행기관에 대한 설문조사에서는 25% 이하의 사건에서 디지털 증거를 포함한다고 나타났다. 이에 대해 지역경찰은 디지털 증거에 대한 훈련 등의 부족으로 인한 충분한 지식과 능력이 없기 때문에 전통적인 증거와 문서 기반의 증거에 집중한다는 것으로, 이는 결과적으로 범죄대응능력을 저하시킬 수 있는 요인으로 매우 심각한 문제로 지적되고 있다. 미국의 경우 90% 이상의 법집행 자원이 이러한 지역단위의 법집행 기관에 속해 있기 때문에 이러한 문제점은 더욱 심각한 것으로 인식되고 있다. 법조계에서 디지털 증거를 적절하게 취급할 준비가 되어 있지 않다. Losavio 등의 조사에 따르면 일반적으로 판사들은 디지털 증거에 대한 자신들의 지식에 대해 불안감을 가지고 있다고 한다.

이렇듯 디지털 포렌식의 발전을 주도하고 있는 미국의 경우에도 이 분야에 대한 자원의 공급은 수요에 크게 미치지는 못하고 있는 것으로 인식되고 있다. 이 분야에 대한 연구자, 학생, 민간기업의 실무자 등을 대상으로 한 각 분야별 수요간의 빈도분석을 한 연구결과를 보면 <표 2>와 같이 교육/훈련/자격, 기술, 암호, 데이터 획득 도구, 도구(tools), 법률시스템, 증거간의 상관 관계, 이론/연구, 재정지원 등의 순으로 수요가 빈번한 것으로 나타났다.[50]

<표 2> 디지털 포렌식 관련 수요에 대한 빈도분석

	빈 도	비 율
교육/훈련/자격	32	18
기 술	28	16
암 호	24	14
데이터획 득 도구	22	13
도 구	18	10
법률시스템	16	9
증거간의 상관 관계	11	6
이론/연구	9	5
재정지원	7	4
기 타	6	3

50) M. Rogers, K. Seigfried, The future of computer forensics: a needs analysis survey, Computer & Security(2004), 23, Elsevier, 12-16.

제2절 법 률

1. 디지털 증거의 획득과 관련된 법률 문제

미국은 Electronic Communications Privacy Act, 수정헌법 제4조에 의한 컴퓨터의 압수·수색, 네트워크 전자감시를 위한 the Pen/Trap Statute, the Wiretap Statute 등의 법률을 통해 디지털 증거의 획득과 관련된 절차규정을 선도하고 있다.[51] 이러한 미국 법률의 특징 중의 하나는 컴퓨터와 네트워크와 관련된 증거의 기술적인 특성이나 사이버범죄의 수사상 특성에 대한 충분한 고려가 반영되어 매우 현실적이고 세부적인 법률 규정이 되어 있으며 법원의 판례 또한 기술적인 문제를 포함하여 매우 방대한 문제들에 대해서 세부적인 기준들을 제시하고 있다는 점이다. 예를 들어 Email의 제목(subject) 항목은 TCP 패킷의 헤더 부분에 들어 있지만 그것은 통신의 내용에 해당하므로 다른 헤더정보와 달리 감청(Intercept)의 대상이 되는 것으로 보는 것과 같은 것, 서버관리자가 컴퓨터에 대한 침입을 감시하기 위해 모니터링하다가 발견한 정보를 수사기관에 감청관련법의 위반없이 제공할 수 있도록 하는 것(18 U.S.C §2511(2)(a)(i)), 해킹 피해자가 수사기관에 해당 컴퓨터에 대한 해커의 통신을 도청할 권한을 부여할 수 있도록 하는 것(18 U.S.C. §2511(2)(i) 등이 그러한 예이다.

1994년 법집행을 위한 통신지원법(Communication Assitance for Law Enforcement Act), 2001년 패트리어트법(Patriot Act 2001), 2002년 사이버안전확장법(Cyber Security Enhancement Act) 등은 국가안전 등을 빌미로 수사기관의 권한을 과도하게 확장하여 시민의 헌법적 권리들을 위협한다는 비판이 있기는 하지만 적어도 증거의 획득과정에서 발생하는 법적인 문제의 발생 소지를 상당히 줄이려는 활발한 입법활동이 존재한다.

그렇다고 모든 법적 장치들이 수사의 편의를 위해 제공되는 것은 아니다. 예를 들어 연방 수사절차법(Federal Rules of Criminal Procedure) 제41조에 의해 수사관은 디지털 증거가 아닌 하드웨어가 금제품(contraband), 증거 또는 범죄의 도구나 결과물

51) 임종인·박종환, 사이버범죄방지조약의 절차규정에 관한 연구, Information Security Review, 창간호, 2004. 12면.

일 때 하드웨어 자체를 압수할 수 있다고 법이 허용하고 있다. 이를 엄격히 해석하여 법원은 단순히 컴퓨터 하드웨어가 범죄 증거를 위한 저장장치일 경우에는 하드웨어에 대한 압수를 허용하지 않는다.(United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982)). 보충적으로 컴퓨터 하드웨어를 압수한 후에는 그 현장을 떠나서 증거를 찾기 위한 수색을 할 것이라는 점을 영장 소명 자료에서 분명히 밝혀야 한다는 지침을 제공한다.[52]

이러한 예에서 보듯이 입법가와 사법부, 그리고 이를 법을 집행하는 기관 각각의 디지털 증거 획득 과정을 적절하고 세밀하게 규율하려는 노력들이 실제로 법을 집행하는 법집행관에게는 해야할 것과 하지 말아야할 것을 분명하게 구분하게 하며 법 집행의 대상자들에게 부당한 피해를 입히지 않게 하는데 크게 일조를 하고 있음에는 틀림이 없다.

2. 디지털 증거의 증거능력 문제

미국에서 증거법은 일반적으로 보통법(comman law)을 따르다가 1975년 연방증거법(Federal Rules of Evidence)이 제정되고 많은 주에서도 이를 모델로 입법하여 가장 중요한 법원(法源)이 되고 있다. 일부 국가의 경우처럼 전자적 증거에 대한 포괄적인 입법을 하고 있지 않다.

합법적으로 수집되었음을 전제로 실제로 법정에서 증거가 어떠한 사실을 판단하는데 자료로 활용되기 위해서는 증거는 사건과 관련성이 있어야 하며(relevant), 신뢰할만하여(reliable and credible) 적격하고(competent), 요증 사실을 입증함에 상당하여야(material) 한다[53]. 이중에 디지털 포렌식과 관련된 문제는 주로 적격성의 내용인 신빙성(reliability)에 집중된다고 볼 수 있다. 신빙성의 문제는 다시 증인 적격의 문제, 증인 자격과 내용의 문제, 증거의 진정성 문제, 전문법칙의 적용 여부 등을 들 수 있다. 증인 적격의 문제는 증인이 진실을 말할 수 있는 정신적, 도덕적인 적격에 관한 문제이므

52) CCIPS, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, (http://www.cybercrime.gov/s&smanual2002.htm), July 2002, .

53) D. Shinder, *Scene of The Cybercrime: Computer Forensic Handbook*, Syngress, 2002. pp.548-551.

로 이를 제외한 나머지에 대해서 간략히 살펴보겠다.

가. 증인 자격과 내용의 문제

증인은 자신이 과거에 경험한 사실을 법원에서 진술하는 '일반증인'과 자신의 경험 뿐 아니라 전문지식에 기초한 사실과 의견을 법원에서 진술하는 '전문증인'으로 구분된다[54]. 법과학에서 주로 문제되는 전문증인(expert witness)의 경우 먼저 증언하려는 내용이 전문증인의 증언대상이 될 수 있는 지의 문제, 증언의 신뢰성에 관한 문제, 전문증인의 자격에 관한 문제 등이 증언의 인용가능성을 판단하는 기준이 된다. 미국 연방증거법 제702조는 만약 과학, 기술, 또는 다른 특별한 지식이 사실의 판단자가 증거나 어떠한 쟁점에 있어서 사실을 결정하는데 있어 도움이 된다면 지식, 기술, 경험, 훈련 혹은 교육에 의해 전문가의 자격이 있는 자가 의견을 진술할 수 있도록 정하고 있다.[55] 디지털 포렌식 관련 내용이 쟁점이 된다면 많은 경우 전문적인 지식이나 경험이 없는 일반적인 법관이나 배심원들은 이를 이해할 수 없기 때문에 흔히 전문가 증언이 필요로 하게 되기 때문에 증언하려는 내용이 전문증인의 증언대상이 될 수 있는 지의 문제보다는 증언의 신뢰성에 관한 문제와 전문증인의 자격에 관한 문제 등이 중요하게 된다.

이 문제는 연방증거법이 명시적인 규정을 두고 있지 않으므로 여러 주요한 판결이 판단기준으로 작용을 해오고 있다.

1923년 Frye v. United States 사건[56]에서 유래한 'Frye Test'는 전문가 증언이 근거하고 있는 과학적 기술(scientific technique)이 관련된 과학계에서 '일반적 승인(general acceptance)'을 받고 있는 지를 기준으로 수용여부를 결정하도록 하고 있다 . 이에 반해 1993년 미 대법원의 Daubert v. Merrell Dow Phamarceuticals Inc. 사

54) 권순철, "미국 증거법상 증거능력 체계: 연방증거법(Federal Rules of Evidence)를 중심으로", 대검찰청 해외연구자료, (대검찰청 홈페이지 연구자료실), 2006.

55) Rule 702. Testimony by Experts
If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.

56) 293F.1013 (D.C.Cir1923).

건[57]에서 유래한 이른바 'Daubert ruling'은 먼저 신뢰성 없는 전문가 증언을 배제하는 책임을 법원에 부여하여 법원이 문지기(gatekeeper)의 역할을 수행하여야 한다고 하고, 일반적 승인 외에도 (1) 사용된 이론이나 기술이 검증된 것인지 (2) 전문적 출판물에 의해 과학계의 검토를 받은 것인지 (3) 잠재적 오류의 비율 등이 검토될 것을 요구한다.[58]

Daubert 기준은 Kumho Tire Company, Ltd. v. Patrick Carmichael 사건[59]을 통해 과학이 아닌 기술적이거나 다른 전문화된 증언에까지 확대되었다. 1989년 People v. Castro 사건[60]에서는 일반적으로 DNA를 이용한 개인식별 기술과 실험이 일반적으로 과학계에서 받아들여지지만 해당 사건에서 일부 과학적 기술과 실험의 방법이 신뢰할 만한 결과를 얻는데 실패하였다며 Frye 요건을 강화하였는데 이는 Frye Plus Test라고 한다. 한편 <표 3>[61]에서 보는 것과 같이 미국의 각 주별 적용하고 있는 판단 기준은 다양하다.

<표 3> 미국의 주별 전문가 증언의 수용여부에 관한 판단기준

Daubert 기준을 사용하는 주	Frye 기준을 사용하는 주	Fyre-Plus 기준을 포함 자체적인 기준을 적용하는 주
Connecticut	Alaska	Arkansas
Indiana	Arizona	Delaware
Kentucky	California	Georgia
Louisiana	Colorado	Iowa
Massachusetts	Florida	Military
Missouri	Illinois	Minnesota
New Mexico	Kansas	Montana

57) 509 U.S. 579 (1993).
58) P. Rice, *Electronic Evidence: Law and Practice*, American Bar Association, 2005. p.322.
59) 526 U.S. 137 (1999).
60) 144 Misc 2d 306 (1989).
61) T. Owen, et. al., "*Law and The Expert Witness-The Admissibility of Recorded Evidence*", AES 26th International Confernece, (http://www.owlinvestigations.com/LawandtheExpertWitnessDenver05paper.pdf), July 2005

Oklahoma South Dakota Texas West Virginia	Maryland Michigan Nebraska New York Pennsylvania Washington	North Carolina Oregon Utah Vermont Wyoming

이러한 문제는 디지털 증거의 검사와 분석, 해석에 있어서 적용되는 이론과 기술, 그것을 다루는 사람의 자격 등이 그 요건에 따라 상당한 신빙성을 제공할 수준에 이르러야 할 것을 요구하는 것이라고 할 수 있다.

나. 증거의 진정성 문제

일반적으로 증거의 진정성(authentication)은 물적 증거의 경우 본래의 그 증거가 맞는지 서류증거의 경우 그에 덧붙여 그 문서가 작성자에 의해 작성된 것이 맞는 지 등에 대한 심사를 포함한다. 문제는 디지털 증거가 사실은 0과 1만으로 이루어진 조합에 불과하지만, 작성자와 내용이 있는 서류와도 같고, 실제로는 하드웨어에서 그 정보가 추출되어야 하기 때문에 그것이 단순하게 규정되기 어려운 복잡한 문제라는 점이다.

디지털 증거가 매체에 저장되어 이동된 경우 이러한 점에서는 실물증거처럼 증거물에 일련번호를 붙이거나 사진을 촬영하는 등의 문서화(documentation) 조치나 증거연계기록(chain of custody)를 유지하는 등의 보존(preservation) 과정상의 절차적 대책이 이행되어야 한다. 일반적으로 기록으로서의 디지털 증거는 연방증거법 제901조(b)(9)에 의해 그 기록을 작성한 프로세스나 시스템에 관한 증거에 의해 진정이 성립된다. 기록내용의 정확성 등의 문제에 있어 전문증인에의한 증언이 필요할 수도 있다. 하지만 진정성을 증명하는 정도에서는 증명해야할 관련사실에 관해 일차적인 정보로 충분하지 자신이 프로그래머가 되거나 심지어 기술적인 작업을 이해할 필요도 없다.[62]

62) CCIPS, *Ibid.*

다. 전문법칙의 예외의 적용여부

대부분의 법원은 컴퓨터 기록을 잠재적인 전문증거로 다루었으나 컴퓨터 기록의 특성을 고려하여 Email처럼 사람이 작성하여 이를 컴퓨터에 저장되기만 한 기록(computer-stored evidence), ATM 영수증 등 컴퓨터에서 생산된 기록(computer-generated ecord), 돈 계산을 위한 스프레드쉬트 프로그램을 사용한 경우처럼 컴퓨터에서 생산함과 동시에 저장된 기록으로 세밀하게 구별하여 컴퓨터에 저장된 기록은 전문증거로, 컴퓨터에서 생산된 기록은 전문법칙의 예외사유인 정기적인 업무활동의 생산기록(연방증거법 제803조 제6호)으로 취급하고 있다. 다만, 이러한 경우에도 그 기록을 작성한 기계가 신뢰할만한 하여 진정성이 인정되어야 한다.

라. 최량증거법칙(Best Evidence Rule)의 적용여부

최량증거법칙은 서류증거의 경우 원칙적으로 원본이 제출되어야 한다는 원칙이다. 하지만 디지털 증거의 경우 원본이라고 하는 것은 가독성이 없는 0과 1의 집합에 불과한 것이기 때문에 이 원칙을 적용하기 곤란한데, 미국의 경우 연방증거법 제1001조 제3호에서 '데이터가 컴퓨터 또는 동종의 기억장치에 축적되어 있는 경우에는 가시성을 가지도록 출력된 인쇄물 기타 산출물로서 데이터의 내용을 정확히 반영하고 있다고 인정되어지는 것은 원본이다'고 규정하여 입법적으로 해결하고 있다.

마. 미국 증거법의 함의

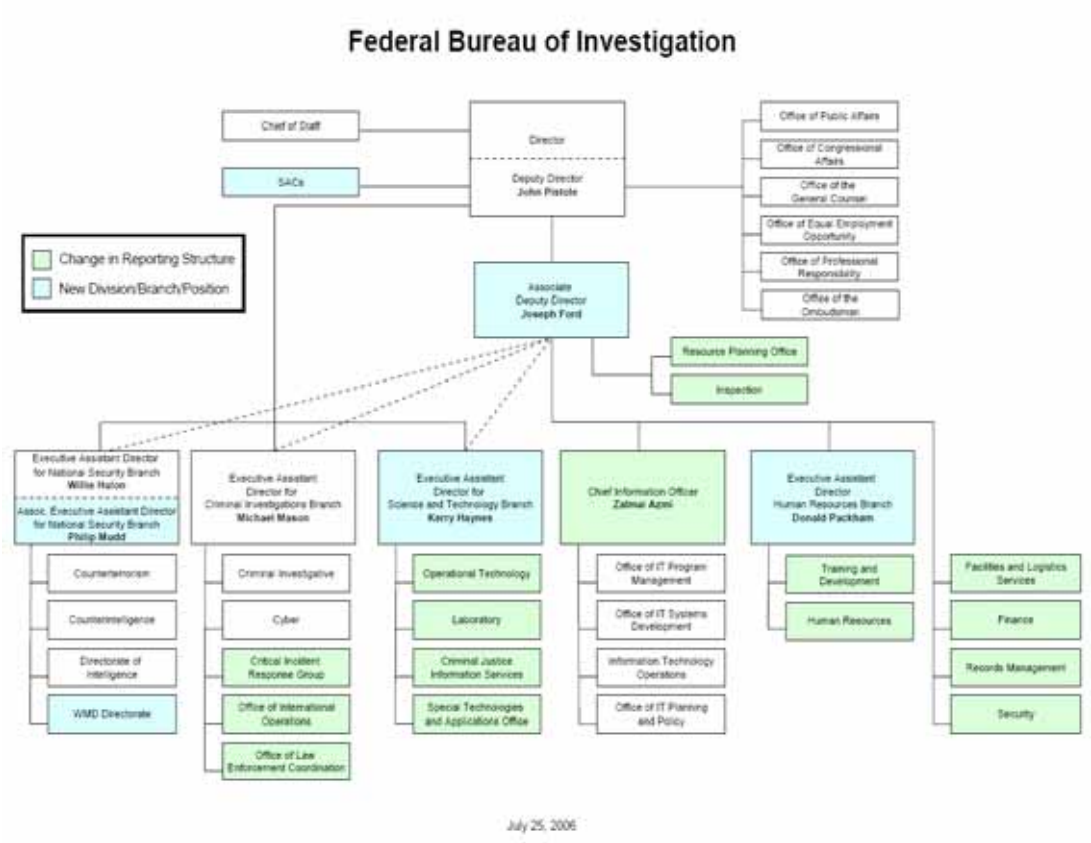
디지털 증거의 증거능력에 대해 포괄적인 입법은 없지만 법정에서의 많은 문제제기로 축적된 판례에 의해 일정한 정도의 기준이 마련되고 있다고 볼 수 있다. 이러한 기준에 의해 디지털 포렌식은 증거의 발견과 수집 단계로부터 보관, 검사, 분석를 거쳐 보고 및 증언에 이르기까지 과학적인 측면에서 다른 법과학과 일부는 공통되며 일부는 독특한 절차와 원칙의 수립과 준수, 이를 취급하는 사람의 전문적 자격의 획득, 도구의 신뢰성 확보, 포렌식랩 등 장소의 안전성 확보를 포함하여 매우 광범위한 부분에서 도전과제를 제시하고 있다고 하겠다.

제3절 디지털 포렌식 관련 조직의 운영

1. 개 요

앞서 살펴본 바와 같이 초창기 수사관들에게 의해 직접 이루어지던 디지털 증거의 처리업무는 현재 디지털 포렌식랩으로 중심이 옮겨지고 있다. 하지만 디지털 포렌식랩의 운영형태는 일반적인 포렌식랩에서 한 하위분야로 다루어지는 경우, 디지털 포렌식랩만이 독립적으로 설치된 경우, 사이버수사 기능의 일부분으로서 포렌식랩을 운영하는 경우, 별도의 포렌식랩을 운영하지 않고 수사기능에서 포렌식 기능을 병행하는 경우 등 매우 다양하다.

FBI Digital Forensic LAB(CART), 마약수사국 DEA의 Digital Evidence Laboratory를 비롯하여 Secret Service나 군 수사기관 등 연방수사기관의 경우 독립된 디지털 포렌식랩을 운영하고 있는 것이 보통이다. 일반적으로 그것을 감당할 수 있는 충분한 자원과 예산, 랩을 운영할 수 있는 기반 체제의 구축 등이 연방기관에 좀 더 용이하다고 볼 때, 디지털 포렌식랩을 분리하여 독립하여 설치하는 것이 좀 더 발전된 형태의 조직 운영 방식이라고 볼 수 있겠다. 참고로 <그림 5>의 FBI의 조직도에서 보듯이 실제 주요 사이버범죄 사건을 처리하는 사이버부(Cyber Division) 등 수사부서와 디지털 포렌식 등 포렌식 업무를 수행하는 OTD 및 Laboratory는 서로 별개의 하위조직에 속한 것을 살펴볼 수 있다.



<그림 5> FBI 조직도 (출처: http://www.fbi.gov/page2/july06/orgchart072606.pdf)

통상 일정 규모 이상의 포렌식랩 조직은 자체적으로 범죄현장을 조사하는 인력과 조직을 보유하고 있기도 한데 이러한 현장경험은 정밀한 증거물의 분석에도 크게 도움이 되는 것이다.

미국 사법통계국의 조사에 따르면 2002년도에 전국에 351개의 공적 포렌식랩이 있는데 이중에 평균 11%의 포렌식랩에서 컴퓨터범죄에 대한 증거분석 업무를 수행하고 있다고 한다.[63] 한편 2000년도 통계에 따르면 미국에는 17,784개의 법집행기관에 796,518명의 법집행관(officer)이 근무하고 있는데,[64] 연방기관을 제외한 주(州)와 지

63) Bureau of Justice Statistics, *Census of Publicly Funded Forensic Crime Laboratories, 2002* (http://www.ojp.usdoj.gov/bjs/pub/pdf/cpffcl02.pdf), 2005.
64) B. Reaves and M. Hickman, *Census of state and local law enforcement agencies, 2000,*

역 단위의 법집행기관을 대상으로 한 조사에서 72.3%의 법집행기관에 전문적인 디지털 증거 부서가 없다고 답했다. 대신 응답자의 33%가 기관 내에 디지털 증거 업무에 종사하는 사람이 있다고 했으며, 대부분의 경우 디지털 증거 분석과 수사업무를 병행한다고 하였다.[65] 2005년의 국립사법연구소의 설문조사에서도 72% 이하의 법집행기관에 디지털 증거 부서가 없으며 절반 이하의 응답자들이 디지털 증거 훈련을 받은 직원들이 있다고 답해 수년간 상황이 크게 변화하지 않은 것으로 나타났다.[66]

이러한 문제들을 해결하기 위한 방안 중 독특한 것이 FBI를 중심으로 각 지방에 속한 법집행기관이 많은 비용이 들어가는 포렌식랩을 개별적으로 설치하기 보다는 연방자금으로 이를 설립하여 공동으로 이용하는 프로그램인 Regional Computer Forensic Laboratory(RCFL)이다. 미국의 연방·주·지역 단위의 다양한 법집행기관에서 행해지는 디지털 포렌식랩의 운영상황을 모두 파악하는 것은 매우 어렵기 때문에 RCFL을 중심으로 랩의 운영실태를 살펴보겠다.

2. Regional Computer Forensic Laboratory(RCFL)

2007년 발간된 2006년 회계년도에 RCFL의 연례보고서를 중심으로 살펴보았다.

가. 운영형태

RCFL 사업은 FBI의 Operational Technology Division에서 담당하며 2002년 설치된 National Program Office에서 이를 관장한다. 1999년 시범사업을 시작으로 2007년 10월 현재 미국 내에는 샌디애고 등 13개 RCFL을 두고 있다. 전국적으로

Bureau of Justice Statistics Bulletin, NCJ 194066, U.S. Department of Justice, Washington, DC (www.ojp.usdoj.gov/bjs/pub/pdf/cslleaOO.pdf), 2002.

65) E. Appel and M. Pollitt, *Report on the Digital Evidence Needs Survery of State, Local, and Tribal Law Enforcement,* (http://www.jciac.org/docs/Digital%20Evidence%20Survey%20Report.pdf), 2005.

66) Regional Computer Forensic Laboratory, *RCFL Program Annual Report for Fiscal Year 2006*, (http://www.rcfl.gov/downloads/documents/RCFL_Nat_Annual06.pdf), 2007

4,321개 법집행기관이 이를 이용할 수 있으며 100개 가량의 기관에서 운영에 참여하고 있다.

RCFL의 주요 임무는 객관적이고 독립적인 디지털 증거검사 업무와 압수수색 지원, 그리고 교육훈련이다. RCFL의 검사관이 되기 위해서는 후술하는 FBI의 CART Forensic Examiner 자격을 취득해야 한다.

나. 인 력

미국의 경우에도 사법연구소(NIJ)와 보안기술연구소(the Institute for Security Technology Studies, ISTS)의 연구[67]에 따르면 좀 더 많은 컴퓨터 범죄 수사관과 기술 및 장비가 필요한 것으로 확인되었다. 디지털 법과학 분야에서도 또한 보다 많은 인력이 필요하지만 상대적으로 적은 근무시간과 많은 보수에 이끌려 고급 수사관들이 민간 분야로 옮겨가 인력 부족이 심화되고 있다.[68] 하지만 현재 CART와 RCFL 등 FBI에 속한 Forensic Examiner만도 300여 명에 이르고 있다. 통상 RCFL에는 FBI측 검사관 3명 가량과 다른 법집행기관 검사관 9명 가량이 활동하고 있다.

다. 예산

2006 회계년도에 RCFL 운영에 사용된 예산은 8,858,949 달러에 이른다. 이중에는 순수 운영비는 55% 가량이고, 교육훈련 19%, 새 RCFL 설립에 5%, 임차료로 21%가 사용되었다. 검사관 개인별 기초 장비는 대략 26,000 달러에 이르며 휴대전화, PDA, 비디오 및 Linux와 Macintosh 등 특별한 운영체제를 담당하는 검사관에게는 추가적인 장비와 소프트웨어가 지급된다. FBI 전체적으로 볼 때 2008 회계연도 FBI의 인터넷, 컴퓨터 및 네트워크 기반의 수사에 500만불, 디지털증거의 수집과 분석(CART)에는 2

67) Institute for Security Technology Studies, *"Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report"* (http://www.ists.dartmouth.edu/TAG/gar/ISTSGapAnalysis2004.pdf), 2004.

68) NIJ, *Status and Needs of Forensic Science Service Providers: A Report to Congress,* (http://www.ncjrs.gov/pdffiles1/nij/213420.pdf), March 2006.

천 2백만불, RCFL에는 6백만불의 예산이 배정되어 있다.[69]

라. 시 설

RCFL에는 공통적으로 증거접수실(Evidence Intake), 복제 전용으로 사용되는 Imaging Room, Storage Area Network(SAN) 장비, 증거분석실(Laboratory/Processing), 검토실(Review Room), 교육장(Training Room) 등을 갖추고 있다. 모든 증거이미지와 분석결과는 SAN 장비에 저장되며 CAIR(Case Agent Investigative Review) 시스템에 의해 분석결과는 온라인을 통해 의뢰기관에 제공된다.

마. 활동실적

2006년 회계년도의 경우 RCFL에 실제로 증거분석을 의뢰한 경우는 800개 이상의 기관에서 4,214건에 달한다. FBI의 자체적인 수사에 활용되는 CART와 달리 RCFL은 연방 뿐 아니라 지방의 모든 법집행 기관에서 참여 및 이용이 가능하다는 특징이 있다.

활동실적의 해마다 크게 증가하고 있다. 이는 서비스 요청, 검사의뢰된 매체의 수, 디지털 증거의 분량, 현장지원을 나간 횟수 등 모든 통계에서 나타나고 있다.

<표 4> RCFL의 연도별 주요 활동실적

활 동 별	2003	2004	2005	2006
서비스 요청(건)	1,444	1,548	3,434	4,214
디지털 포렌식 검사 (매체수)	987	1,304	2,977	3,633
처리된 디지털 증거 분량(테라바이트)	82.3	229	457	916
현장 지원(건)	196	177	288	803

포렌식 검사 의뢰가 들어온 매체의 형태는 매우 다양하다. 국내에서는 이제 소수만이 사용하는 플로피 디스크로부터 휴대전화나 CPU와 같은 장치에 이르기까지 다양하다.

69) Andrew Noyes, *"FBI's budget chock-full of tech-related efforts"*, (http://www.govexec.com/story_page.cfm?articleid=37817), August 20, 2007

<표 5> RCFL의 2006 회계연도 매체별 증거분석량

매체 유형	수 량
CD	20,960
Cellular Telephone	701
Devices (e.g., CPUs)	75
DVD	2,494
Flash Media	1,142
Floppy	16,019
HDD	15,079
Magneto Optical	48
Other	1,429
PDA	97
Tape	648
Zip/Jazz/Super Disc	985
Total	59,677

3. Computer Analysis Response Team

FBI의 CART는 FBI와 지역사무소의 자체 사건처리에 활용되기 때문에 그 구성 등이 정밀하게 보고된 것은 없다. 2008년 CART 예산 신청 현황을 보면 4명의 특별수사관을 포함한 54개의 보직이 있고, 인건비를 제외하고 22,840,000달러, 인건비 포함 42,575,000 달러 규모이다.[70] 한편 미 법무부의 감사보고서[71]에 따르면 CART내에는

70) US Department of Justice, *2008 Budget and Performance Summary,* (http://www.usdoj.gov/jmd/2008summary/html/107_fbi.htm), 2007.

71) US Department of Justice, *Audit of the Department Justice Information Technology Studies, Plans, and Evaluations*, (http://www.usdoj.gov/oig/reports/plus/a0739/final.pdf), August 2007.

중앙집중식 증거저장 장치인 CARTSAN(CART Storage Area Network)이 설치되어 있는데 2001년 시작된 CARTSAN 설치 프로젝트는 2005년에 승인 및 인증을 받았고 2006년까지 25개의 CART와 RCFL에 설치가 되었으며 2007년부터 다시 25개를 설치할 계획으로 있다. 2006 회계년도에 CART는 10,000건의 컴퓨터 매체에 대한 검사를 통해 1 페타바이트 분량의 데이터를 CARTSAN을 통해 처리한 것으로 추산하고 있다. 2003년의 CART의 사건처리량은 6,500건 가량에 782 테라바이트 분량이었다[72]. <표 6>은 위 감사보고서에 나타난 CARTSAN의 대한 연구, 계획, 평가 과정의 부분으로, 이러한 저장장치 등 포렌식과 관련된 IT 기반이 얼마나 엄격하게 설치, 관리되고 있는지 보여준다고 하겠다.

<표 6> CARTSAN 연구, 계획, 평가

문서형태	제 목	날 짜
경영 사례 연구	OMB Exhibit 300 for BY 2008	2006.12
프라이버시 영향평가	Privacy Impact Assessment, CARTSAN, (Draft)	
위험관리 계획	위험관리 계획	2005.7
보안 계획	시스템보안계획, CARTSAN	2005.8
구성(configuration) 관리 계획	구성관리계획, Version 0.1 (Draft)	
품질 보증 계획	디지털 증거랩 품질보증 매뉴얼 보충, CART	2006.4
시험 계획	공인시험보고서, CARTSAN	2005.8
설치 계획	CARTSAN 검토 네트워크 설치 계획	2005.6
시험 보고	공인시험보고서, CARTSAN	2005.8
성능 평가	획득자산 관리표	2005.6
성능 평가	투자관리/프로젝트 검토 위원회	2005.8

72) The History of Computer Forensics (http://www.pc-history.org/forensics.htm) 참조.

제4절 포렌식랩 인증

디지털 포렌식 분야에서는 통일된 표준과 적격성에 대한 목록이 없기 때문에 실무자에 대한 자격과 훈련 및 포렌식랩의 인증에 있어서 문제점이 있다는 지적이 있었다.[73] 그러나 결국 SWGDE 등의 노력에 힘입어 2003년 4월 디지털 포렌식은 ASCLD/LAB의 인증프로그램에 포함되었다. 이에 따라 4개의 하위분야(오디오 분석, 컴퓨터 포렌식, 디지털 이미징 분석, 비디오 분석) 중 어느 하나라도 취급하는 포렌식랩은 디지털 증거를 취급하는 기관으로 인증을 신청해야 한다.[74] 이것은 어찌 보면 매우 놀라운 결과인데, ASCLD/LAB이 개별적으로 인증 요건을 정하고 있는 법과학 분야는 그 이전까지 통제물질, 독물학, 미세증거, 생물학, 무기와 도구흔, 문서, 잠재지문, 기술지원, 범죄현장 등 분야에 한정되고 있었기 때문이다. 이를 통해 디지털 포렌식은 정규적인 법과학의 한 분야로 인정받는 계기가 되었다는데 큰 의미가 있으며 이는 디지털 포렌식에 대한 통일된 표준 및 적격성 등 여러 사항에 대한 연구와 합의가 매우 빠른 시간 내에 이루어졌다는 것을 뜻한다고 볼 수 있다. ASCLD/LAB의 인증요건은 인증매뉴얼에서 그 내용을 살펴볼 수 있는데 그 내용이 방대하므로 본문에 포함하지 않고 발췌번역문을 부록으로 덧붙였다.

2004년 North Texas RCFL은 최초의 ASCLD/LAB 인증을 받은 연방 디지털 증거 시설이 되었고, FBI OTD (Operational Technology Division)의 Digital Evidence Laboratory(DEL)은 2007. 6 디지털과 멀티미디어 증거(D&ME) 전 분야에서 ASCLD 국제 인증(International Accreditation)을 받은 최초의 랩이 되었다.[75] 다른 연방기관으로는 마약수사국(DEA)의 Digital Evidence Laboratory, 지방 법집행기관으로는 Charleston 경찰국의 Digital Evidence Unit Laboratory 등이 최근 ASCLD/LAB 인증을 받았다.[76]

---

73) M. Meyers, M. Rogers, "*Computer Forensics: The Need for Standardization and Certification*", International Journal of Digital Evidence, 3(2), 2004.
74) J. Barbara, "*Digital Evidence Accreditation*", Forensic Magazine, (http://www.forensicmag.com/articles.asp?pid=21), Winter 2004.
75) http://www.fbi.gov/pressrel/pressrel07/accretitation060707.htm 참조
76) http://www.ascld-lab.org/legacy/aslablegacylaboratories.html 참조

아직 많은 포렌식랩에서 인증을 받지 못하고 있지만 디지털 포렌식랩에서의 시험결과에 대한 신뢰성을 확보하기 위한 여러 하위요소들을 제3자가 평가하여 이를 공인하여 주는 인증제도가 포렌식랩의 뚜렷한 설치 및 운영방향을 제시해주며 많은 포렌식랩에서 인증을 받는 것을 목표로 삼고 있음은 분명하다.

제5절 교육・훈련・자격제도

미국에서 훈련받는 디지털 포렌식 전문가에 대한 수요가 폭발적이며, 심지어 전통적으로 이 분야의 수요를 창출하고 발전시키는데 중요한 기여를 했던 법집행기관에서는 상대적으로 낮은 보수 등으로 인력부족이 심각하다. 퍼듀대학교와 같이 잘 알려진 디지털 포렌식 과정을 졸업한 학생(석사)들은 최초 85만에서 100만 달러의 연봉을 제시받으며, 그렇지 못한 대학들도 50만에서 60만에서 시작하지만 3,4년 안에 150만 달러 가까이 연봉이 증가한다고 한다[77]. 이러한 상황은 미국에는 디지털 포렌식에 대한 대학에서의 교육을 폭발적으로 증가시키고 있어 이미 2006년도에 그 수가 100여개 코스에 이른다고 한다.[78] 그 목록의 일부는 E-evidence Information Center 웹사이트에서 확인할 수 있다.[79] 일반적으로 대학에서의 교육은 컴퓨터 공학, 형사정책(Criminal Justice), 경영학 과정 등에서 한두 개의 일반적인 코스를 제공하거나 자격 혹은 석사과정에서 예닐곱 개의 집중적 과정을 제공하는 형태로 진행된다.

대학 외의 포렌식 훈련은 특정한 소프트웨어 업체의 훈련, 산업계의 훈련, 또한 전문기관의 훈련 등으로 구분될 수 있다. 이러한 교육과 훈련제도에서 가장 큰 쟁점은 누가 급변하는 디지털 포렌식 분야를 전문가를 양성해야 하며, 어떠한 표준이 적용되어야 하는 것이다.

---

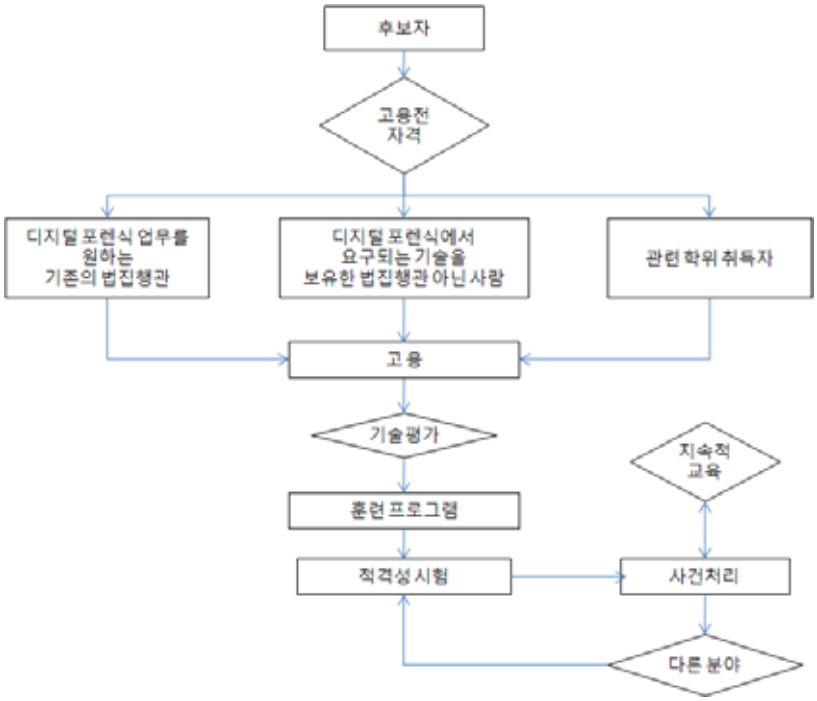
77) C. Taylor, B. Endicott-Popovsky, A. Phillips, "*Forensics Education: Assessment and Measures of Excellence",* proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2007), 155-165, 2007.

78) http://www.usatoday.com/tech/news/techinnovations/2006-06-05-digital-forensics_x.htm. 참조

79) http://www.e-evidence.info/education.html 참조.

1. 교 육

앞서 언급한 것과 같이 미국에서는 국립사법연구소를 중심으로 법과학 교육 품질을 향상시키기 위한 노력을 경주하고 있다. 2004년의 법과학 교육을 위한 TWGED의 가이드라인에 포함시키지 못한 디지털 포렌식 분야에 대한 교육훈련을 위한 TWGDE (Technical Working Group for Education and Training in Digital Forensics)의 보고서는 작성되어 국립사법연구소에서 출간을 기다리고 있다.[80] 동 보고서에서 디지털 포렌식 실무가의 경력개발의 경로는 <그림 6>과 같다. 이에 따르면 디지털 포렌식 실무자가 되기 위한 지원자는 세가지의 경로를 따를 수 있는데, 기존의 법집행관, 법집행관이 아니지만 기술이 있는 사람, 학위를 지닌 사람 등이다. 하지만 그 경로와 관계없이 개인적 염결성(integrity)과 함께 지식, 기술, 능력(Knowledge, Skills, Abilities, KSAs)를 지니고 있어야 한다.



<그림 6> 디지털 포렌식 실무자의 경력개발

80) 동 보고서는 http://www.aafs.org/pdf/NIJReport.pdf 참조.

개인적 염결성(integrity)과 관련된 개인특성의 요구사항은 앞서 제시된 일반 법과학의 경우와 같다. 대학교육(academic qualification) 측면에서 역사적으로 디지털 포렌식 분야에서는 학위를 요구하지 않았지만 점차 추세는 학위, 특히 과학 분야에대한 학위를 요구하는 것으로 바뀌고 있다. 참고로 ASCLD/LAB 인증요건에 부합하려면 디지털 포렌식 실무자들은 최소한 자연과학 분야의 학사학위를 지니고 있어야 한다.

기술적, 전문적으로 요구되는 사항들은 <표 7>와 같다.

<표 7> 디지털 포렌식 실무가에게 요구되는 기술적, 전문적 능력

기술적 요건	전문적 요건
• 컴퓨터하드웨어와 아키텍처(Computer hardware and architecture) • 저장매체 (Storage media) • 운영체제(Operating systems) • 파일시스템(File systems) • 데이터베이스 시스템(Database systems) • 네트워크 기술과 정보통신기반(Network technologies and infrastructures) • 프로그래밍과 스크립팅(Programming and scripting) • 컴퓨터 보안(Computer security) • 암호(Cryptography) • 소프트웨어 도구(Software tools) • 검증과 시험(Validation and testing) • 타분야에 대한 인식(Cross discipline awareness)	• 비판적사고(Critical thinking) • 과학방법론(Scientific methodology) • 정량적 추리와 문제해결(Quantitative reasoning and problem solving) • 의사결정(Decision making) • 랩실무(Laboratory practices) • 랩안전(Laboratory safety) • 세부사항에 대한 주의(Attention to detail) • 대인기술(Interpersonal skills) • 공적말하기(Public speaking) • 구두,서면 커뮤니케이션(Oral and written communication) • 시간관리(Time management) • 작업우선선위선정(Task prioritization) • 디지털포렌식 절차의 응용(Application of digital forensic procedures) • 증거보존(Preservation of evidence) • 검사결과의 해석(Interpretation of examination results) • 수사절차(Investigative process) • 법절차(Legal process)

동 보고서에서는 검토사항을 토대로 2년제 전문대 연계 과정(associate degree), 학

사 학위과정, 대학원 과정, 대학에서의 자격공인 과정, 훈련 및 계속 교육으로부터 각 교육의 커리큘럼과 교육에 필요한 자원등 요구사항을 기술하고 있다. 이 중에 다른 과정과 달리 학사과정의 경우 구체화된 모델 커리큘럼을 제시하고 있는데 그 내용은 <표 8>과 같다.

<표 8> 디지털 포렌식 학부과정 커리큘럼 모델

구 분	과 목
대학 일반 교육 (36-40 학점)	대학의 요구사항에 따라 언어, 인성, 사회과학, 수학, 공적 연설 등을 포함할 수 있음 학생들이 과학 방법론과 전자기학 기초를 접할 수 있는 6학점의 과학코스가 여기에 포함되어야 함 일부 컴퓨터 포렌식 과학/디지털 증거 학위 코스는 이 요구를 충족할 수 있음
핵심 컴퓨터 및 정보과학 (24 학점)	컴퓨터와 저장매체 개론, 응용 파일시스템과 운영체제 기초 컴퓨터 네트워킹과 네트워크 보안, 프로그래밍 I, 컴퓨터 아키텍쳐 데이터베이스/응용프로그램 정보 보안, 이산수학
핵심 법과학 (6 학점)	법과학개론 법과학 전문 실무a
추가적 필수코스 (16 학점) (일부는 일반 대학 과정 교육을 대체할 수 있음)	기초 법률 문제(증거), 범죄수사, 공적 연설, 기술적인 글쓰기, 졸업 프로젝트(Capstone Project) 디지털 포렌식의 쟁점 (1 학점 세미나)
핵심 디지털 포렌식랩 (12 학점)	기초 컴퓨터 포렌식(3학점 + 1시간 실습) 파일시스템과 운영체제 증거복구와 검사(3학점 + 1시간 실습) 디지털 매체, 저장 장치와 응용프로그램 분석(3학점 + 1시간 실습)
상급 포렌식 코스	
고급 핵심 디지털 포렌식 (필수: 11 학점)	고급 컴퓨터 포렌식(3학점 + 1시간 실습), 네트워크 포렌식(3학점 + 1시간 실습) 저장 시스템(3학점)
기술 선택 (필수: 9 학점)	개인 전자장치(PED) 포렌식(3학점 + 1시간 실습) 임베디드 장치 포렌식(3학점 + 1시간 실습) 사고대응(3학점) 역공학기술과 대응(3학점) 멀티미디어 포렌식(3학점) 통계학(3학점) 개별 연구(3학점) 디지털 포렌식의 고급 법률 문제(3학점) 민사법문제(3학점)
대학 일반 선택 (6 학점)	자유선택(인턴쉽 포함 가능)
a. 이 과정은 윤리, 법정 증언, 증거, 증거연계관리(chain of custody), 안전 등을 포함함. b. 여기서 기재된 선택과목은 한정되는 것이 아니라 관심 분야에 따라 조정될 수 있음	

대학원 과정은 경우 커리큘럼은 교육기관의 임무나 시설, 관심과 학생과 교수의 능력에 따라 다를 수 있으며 연구 프로젝트에의 참여가 권장되고 있다. 커리큘럼에 포함될 수 있는 영역에 대한 분류는 <표 9>과 같다.

<표 9> 대학원 과정의 커리큘럼 모델

구 분	내 용
디지털 포렌식 방법론 개발	· 단일 혹은 다중의 장치나 시스템을 포함한 복잡한 시나리오를 받아 이에 대한 해결방안을 제안, 개발, 검증하는 것
고급 운영체제 분석	· 실시간 시스템 · 트랜잭션 처리 시스템
디지털 포렌식 행정	· 범죄현장 관리 · 포렌식랩 관리 · 사건관리 · 품질보증(Quality assurance) · 윤리 및 전문가 책임
증거보존	· 통제와 검증 절차 · 증거역학: 보존에 있어 자연, 인간, 도구, 시간의 영향과 디지털 증거의 복구
민·형사법률문제	· 법정증언 · 법정에의 증거제출 · 고급 법률문제/규제 · 컴퓨터 압수수색 · 모의재판 · Electronic Discovery · 증거법
복잡(Complex) 데이터 분석	· 관계분석 · 디지털 증거와 물리적 증거의 연결 · 시계열 분석: 데이터와 관련된 날짜와 시간의 상관관계 · Understanding Data Structures
복잡 사례연구 /시뮬레이션	· 상관관계를 확인하기 위한 다량의 사건에서의 디지털 증거의 비교 · 대량 데이터 세트에 대한 검사 · 기업 시스템 · 중복 관할과 국제 수사에 있어 증거 문제
데이터 통신과 네트워크 시스템	· 패킷과 프레임 분석 · 네트워크 보안의 이해 · 네트워크 트래픽 재구성과 추적

컴퓨터 포렌식 분야는 과학적 분야로 인식되기 위한 교차점에 있다.[81] 아직 대학과

81) M. Rogers, K. Seigfried, The future of computer forensics: a needs analysis survey,

대학원 과정에 대한 FEDAC 등의 인증절차는 확립되지 않았으며 인증이 이루어지지 않고 있다. 따라서 실제로 대학에서 이루어지는 교육의 커리큘럼은 다소간 차이가 있을 수 있다. <표 10>에서는 미국 미주리남부대학 컴퓨터정보과학 및 형사사법과학(컴퓨터포렌식 옵션) 학사과정 커리큘럼을, <표 11>에서 퍼듀대학교 사이버포렌식 석사과정 커리큘럼을 정리하였다.

<표 10> 미주리남부대학(MSSU) 컴퓨터정보과학 및 형사사법과학(컴퓨터포렌식 옵션) 학사과정 커리큘럼

1학년		**2학년**	
1학기	학점	1학기	학점
프로그래밍 I	3	DBMS I	3
범죄수사 I	3	컴퓨터 네트워크	3
대수학	3	형사법	3
영작 I	3	인터뷰와 보고서 작성	3
Lifetime Wellness	2	물리학 개론	5
오리엔테이션	1		
2학기		**2학기**	
프로그래밍 II	3	정보시스템 I	3
형사절차	3	데이터 구조론	3
미국경제	3	범죄수사론 II	3
영작 II (WI)	3	체육	1
생물학	4	화법	3
		일반 선택	3
3학년		**4학년**	
1학기	학점	1학기	학점
UNIX 시스템 관리	3	운영체제	3
정보시스템 II	3	선택과목	3
자산보호	3	국제관계	3
문학과 인성	3	미국사	3
미국사	3	선택과목	3
2학기		2학기	
컴퓨터 포렌식	3	DBMS II	3
선택과목	3	선택과목	3
선택과목	3	선택과목	3
문학	3	예술	3
일반 심리학	3	미국 정부조직	3
		전체	**124**

(출처: http://www.mssu.edu/schtech/criminaljustice/BSForensics.htm)

Computer & Security(2004), 23, Elsevier, 12-16.

<표 11> 퍼듀대 사이버포렌식 석사과정 커리큘럼

전 체	필수과목 (6학점), 전문화(15학점), 선택과목(6시간), 논문(6시간)
필수과목	산업・공학에서의 측정과 평가, 또는 통계, 또는 심리학 (3)
	산업・공학에서의 연구 분석 (3)
전문 과목 (15 hrs)	기초 사이버포렌식 (3)
	사이버포렌식에서 고급 연구 주제 (3)
	소형 디지털 장치 포렌식 (3)
	최신 토픽 (3)
	파일시스템 포렌식 (3)
	전문가 증언 (3)
	필수 하드웨어 필수 (1)

(출처: http://cyberforensics.purdue.edu)

아직까지 100여개에 이르는 미국내 대학에서 디지털 포렌식 관련 교육의 상당수는 학위과정 보다는 법집행관 등 실무자들을 대상으로 한 자격과정인데, 위 보고서에서는 동 자격과정에 대한 커리큘럼과 요건 등에 대해서도 언급하고 있다. 하지만 역시 이러한 자격과정에 대한 인증제도는 아직 존재하지 않는다.

2. 훈련과 지속적 전문성 개발

위 TWGDE의 가이드에 따르면 훈련(training)은 디지털 포렌식 실무자들이 특정한 디지털 포렌식 분석을 수행하는데 요구되는 일정한 수준의 과학적 지식과 경험에 이르게 하는 공식적이고 구조화된 과정이다. 적절한 훈련과 전문성은 개인이 독립적인 사건처리를 할 자격이 주어지기 이전에 필요한 요소이다.

지속적 전문성 개발(continuing professional development)은 현재 상태를 유지하거나 더 높은 전문성, 특기, 혹은 책임의 진보를 가져올 수 있는 체제를 말한다. 조직은 지속적인 전문성 개발에 대한 지원과 기회를 주어야할 지속적 책임이 있다. 이러한 훈려과 전문성 개발과 관련된 사항은 적절하게 문서화되며 항구적으로 보존되어야 한다.

적격성, OJT(on-the-job), 및 지속적인 전문성 개발에 필요한 모델 기준은 핵심요소와 분야별 프로그램으로 구분된다. 핵심요소에는 수행표준(전문가 윤리 훈련 포함), 안

전, 정책, 법률, 증거처리, 커뮤니케이션 등이 포함되며, 분야별 요소에는 분야별 역사, 관련 문학, 방법론과 검증 연구, 하드웨어·소프트웨어·기타 디지털 매체, 관련 분야에 대한 지식, 법정 증언, 특정 범죄형태에 대한 훈련, 법적 측면에 대한 지식 등을 포함한다.

이러한 형태의 계속적인 훈련은 많은 기관에서 의무사항이다. 예를 들어 FBI CART는 연간64시간, ASCLD/LAB은 40시간, IACIS는 연간 60시간의 보수 교육과 자격을 유지하기 위해 매 3년 마다 적격성 시험(competency examination)을 볼 것을 의무화하고 있다.

3. 자격 제도

인증(accreditation)이 포렌식랩에 대한 자격제도라면 개인 또한 자격공인(certification)을 받을 것이 요구된다. 자격제도는 크게 필요로 하는 기관에 의해 직접적으로 훈련과 연계하여 이루어지는 경우, 전문적인 기관에 의해 이루어지는 경우, 특정한 업체가 자사의 제품을 기반으로 하여 인증하는 경우 등 다양하다.

가. 주요 기관의 자격인증 제도

디지털 포렌식 자격위원회 Digital Forensic Certification Board(DFCB)에서 각 기관의 대표자를 대상으로 파악한 주요 연방기관별 자격제도는 다음과 같다.[82]

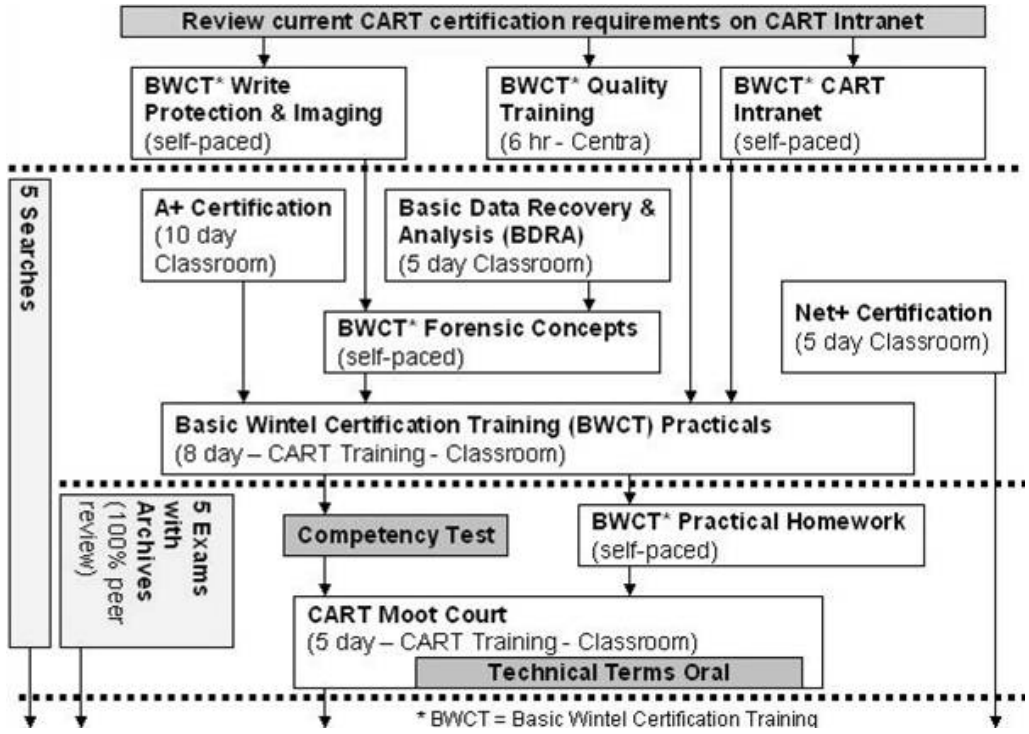
82) The National Center for Forensic Science The Certification Roundtable Meeting, *Draft Final Report,* (http://www.ncfs.org/dfcb/CERT%20ROUNDTABLE%20REPORT%20(DRAFT%20V%206-07-04).pdf.), 2006.

<표 12> 미국 주요기관의 포렌식 검사관 자격제도

조 직	국 세 청(IRS)
자격명	“Computer Investigative Specialist”
응시요건	학사학위(B.A., B.S.) 선임 특수요원, 법죄수사; 13등급
심사방법	3단계 훈련: P-CERT A-CERT (ENCASE, I-LOOK) B-CERT (Networks) 숙련도 시험 : 각 단계의 실기 테스트
갱신 필요	있음
1인당 비용	$30,000
자격을 받은 인원	200
조직	United States Secret Service (USSS)
자격명	Electronic Crime Special Agent Program
응시요건	USSS 특수요원
	학사학위(B.A., B.S.), 2쪽의 질문지
심사방법	기초자격: 최소 연간 30개 시험
	고급자격: 최소 연간 30개 시험
1인당 비용	$80,000
조직	FBI/Cart
자격명	CART Forensic Examiner
응시요건	학사학위를 받은 FBI요원, 지원인력, RCFL 파견자
심사방법	A-plus certification (기초 전산관련 자격시험) Net+ 검정, 기초 데이터 복구, NWCE CART 기초 시험 훈련, OJT, 모의법정, 구술시험, 숙련도 시험, 매년 재심사
갱신 필요	있음 GIAC GCFA (매4년) 자격마다 필기시험
1인당 비용	최초 심사(코스별 $250-500)
	갱신 ($120.00)
자격을 받은 인원	현재 250명, 누적 350명

이러한 자격제도가 생겨난 이유 중에 하나는 수사기관이 능력 있는 검사관 수요를 감당할 수 있는 전문인력을 기존의 대학교육과 일반적인 자격제도 하에서 수급할 수 없었기 때문이다. 이중에 CART의 Forensic Examiner 훈련 및 자격심사를 좀 더 깊이 살펴보겠다.

CART의 Forensic Examiner는 압수수색지원/디지털증거분석/법정증언 등 임무수행의 임무를 수행한다. 훈련과정의 커리큘럼은 <그림 8>과 같다. 자격심사는 Wintel (Windows OS, Intel Architecture)과정에만 7~24개월 소요되며, Unix/Linux, Macintosh, PDA, 휴대전화 등 다른 분야에 대해서는 추가적인 훈련과 심사를 받아야 한다. BWCT(Basic Wintel Certification Training)는 Wintel에 사용가능한 모든 허용된 도구 사용하여 8일간 5개의 시험을 치루며, 이외에도 개별 밀착지도(coaching), 교재를 이용한 개별학습, 개인 탐구활동, 온라인강의, 강의실교육을 병행하는 등 다양한 교육방법을 활용하는 것이 특징이다. 또한 시뮬레이션으로 능력시험(하드드라이브를 주고 증거를 찾는지, 절차를 따르는지, 수사관과의 효과적으로 대화, 법적인 문제에 대응능력, 수사관이 이해하기 쉽게 자료작성) 및 모의법정 심사를 통과해야 한다. 모의법정은 1.5~2시간 가량의 구두 증언으로 이루어진다.



<그림 7> CART forensic examiner certification curriculum (2004. 2월 현재)

FBI에서는 이와 같은 훈련의 성공요건으로서 CART 및 RCFL 등 현장과는 분리된 교육 전담부서가 존재하는 것이 핵심이며, 대신에 그러한 현장부서와 적극적인 의사소통을 통해 현장감 있는 교육을 실시하며 훈련 전문가를 배치하는 것을 꼽고 있다.[83]

나. 전문기관에 의한 자격 제도

소수의 전문기관에 의한 자격 인증 제도가 존재하는데 이러한 자격제도의 특징은 기간이 대체로 짧아 실제로 포렌식 실무가의 적격성을 완전히 판단하는데 활용되기 보다는 최소한의기초수준의 능력을 판단하는데 사용될 수 있다.[84]

<표 13> 주요 전문기관의 포렌식 검사관 자격제도

자 격 명 칭	자격인증 기관	특 징
공인 컴퓨터 검사관 Certified Computer Examiner(CCE)	International Society of Forensics Computer Examiners	· 인정된 훈련과 경력 필요 · 3개 모듈의 필답 및 실기시험 · 현재 가장 널리 알려짐
GIAC 공인 포렌식 분석가 GIAC Certified Forensics Analysist(CFA)	Global Information Assurance Organization	· 75개의 질문으로 이루어진 · 2개의 온라인 시험
공인 컴퓨터 포렌식 기술사 Certified Computer Forensics Technician(CCFT)	High Tech Crime Network	· 공인 컴퓨터범죄 수사관, · 검사, 변호사 등 자격시험 병행
공인 포렌식 컴퓨터 검사관 Certified Forensic Computer Examiner(CFCE)	International Association of Computer Investigators	· 회원, 혹은 실제 데이터를 대상으로 외부 시험 · 2주간의 교육과 병행
사이버보안 포렌식 분석가 Cyber Security Forensics Analyst(CSFA)	Cyber Security Institute	· 제품 중립적인 시험 · 실제 사건 시나리오를 객관식으로 시험

83) A. Corrigan, *How To Make a Forensic Examiner*, 2004 HTCIA International Training Conference & Expo, presentation 자료를 정리한 것임.
84) C. Taylor, B. Endicott-Popovsky, A. Phillips, *Ibid.*

이외에도 Encase나 FTK와 같은 포렌식 제품에 기반한 제조업체에서 운영하는 교육 훈련과 자격제도는 매우 다양하다. 하지만 이러한 자격제도의 범람은 사회적으로 승인된 디지털 포렌식의 핵심 지식과 훈련 및 평가 방법의 부재 등에 기인한 면이 크며, 따라서 이러한 자격들이 실제로 포렌식 실무자들의 적격성을 검증하는데 충분한 것으로 여겨지지 않는다.

이에 따라서 디지털 포렌식 분야에서 국가적인 자격공인 체제에 대한 연구가 국립법과학센터(NCFS)의 디지털 포렌식 자격 위원회(Digital Forensic Certification Board, DFCB)에 의해 진행되고 있다. 이에 근거한 자격인증이 2007년 중에 이루어질 예정이었지만 현재 2008년으로 미루어진 상태이다. DFCB의 자격은 현재 국가(미국)기반의 자격제도이지만 국제적인 자격으로 발전 필요성을 검토 중에 있다.[85]

DFCB에서 제시하고 있는 디지털 포렌식의 핵심적 역량은 기반 지식, 증거획득 지식, 검사 지식, 분석 지식 등으로 구분되며 세부적인 내용은 <표 14>과 같다.

DFCB 증거획득 자격(Acquisition Certification)은 기반 지식, 증거획득 지식, 검사 지식, 분석 지식을 DFCB 검사관 자격(Examiner Certification)은 기반 지식, 증거 획득 지식, DFCB 포렌식 기반 자격(Forensic Foundation Certificate)는 기반 지식을 대상으로 자격 검사를 실시한다.

85) C. Taylor, B. Endicott-Popovsky, A. Phillips, *Ibid.*

<표 14> Digital Forensics Certification Board Core Competencies

구 분	항 목	내 용
기반기술 (Foundation Skills)	품질보증 (Quality Assurance)	검증(validation)/확인(verification) Standard Operating Procedures/Protocols 최적 방법(Best Practice)
	법과 윤리 (Legal and Ethics)	법적 권한/윤리/전문성 개발
	기술(Techniques)	수집/표시/이송/포장/저장
	과정(Process)	범죄현장/사고대응 과정, 전반적인 포렌식 검사 수사/감사/분석 과정, 문서화/보고 및 제출 과정
	Concepts	과학적 방법, 하드웨어, 운영체제, 소프트웨어, 네트워크(구성요소/장비, 구조, 프로토콜, 보호, 인터넷)
증거획득 (acquisition)	Remote/Live/Field/Lab	원격/라이브/현장/랩에서의 수집계획 수립, 증거에 대한 식별, 최우량 사례, 법적인 문제 포함
	QA	법적 권한
	Acquisition Techniques	imaging, wiping, write block, volatile data 등 증거수집에 관련된 지식,기술,역량
	Computer Data Concepts	컴퓨터 데이터와 관련된 주요 개념요소 이해
	Process	수집과정에 대한 포괄적 지식
	다음 사항을 포함 Preview/Minimization, 하드웨어식별, 보존/저장/축적, 미디어 기초, 하드웨어, 메모리구조, 파티션, 파일과 운영체제 데이터 구조, BIOS, 품질보증/통제, 통제, 검증, SOP, 기술한계	
검사 (examination)	Networking과 Communication	Email, 인터넷 분석, P2P, 악성프로그램, 숨겨진 데이터/스테가노그라피, 안티포렌식기술, 암호기술, 검사방법 및 기술, 데이터 확인, 데이터 축소, 디렉토리 리스팅, 삭제된 파일 복구, 흔적 추출, 검색, 데이터 소유와 이력, 파일데이터의 대조
	Special Interest Data	특별한 데이터 형태에 대한 취급
	Exam Techniques	관계있는 정보의 추출기술
	Computer / Data Concepts	운영체제, 파일시스템/구조, 논리 데이터, 메타 데이터, 라이브 데이터, DB와 응용데이터 파일 구조
	Hardware	전자장치에 대한 실질적인 지식
	Exam Process	검사계획, SOPs, 프로토콜과 문서화
분석 (analysis)	Law and Procedures	범죄 구성요소/수사의 초점, 민형사 법과 절차, 특권과 정보 구분 (HIPPA, GLB, FERPA, ECPA 등 관련 법에 따른 정보구분)
	Analytical Techniques	통신 추적, 타임라인 분석, 관계 분석, 화계 분석, 분석 도구 이해, 분석 계획
	Techniques Technology	디지털 증거 메터데이터의 신뢰성, 정보의 외부적 확인, 기초 디스크 구조 이해
	기타: 문서화 및 요구자, 검사관 및 제3자와의 커뮤니케이션	

(출처: http://www.ncfs.org/dfcb/core_competencies.html)

4. 자격제도에 대한 인증

한편 이러한 자격제도는 각 분야별로 다양할 수 있으므로 그 자격제도에 대한 품질과 일관성을 유지할 필요가 있어 그 자격제도 자체에 대한 인증에 대한 필요성이 제기되어 2003년 전미법과학회(American Academy of Forensic Sciences, AAFS), 국립법과학기술센터(National Forensic Science Technology Center, NFSTC), 국립사법연구소(National Institute of Justice, NIJ) 등의 지원으로 포렌식 전문가 인증위원회(Forensic Specialties Accreditation Board, Inc., FSAB)가 설립되었다. 설립 당시 전문적이고 다른 분야에 비해 수요가 많지 않은 포렌식 분야에 대해서는 이를 전담하는 전문적인 인증위원회가 기존의 National Commission of Certifying Agencies(NCCA) 등 자격제도 인증기구와 별도로 설립되어야 한다는 검토가 있었다. 2007. 10월 현재 전미법독성학 위원회 등 6개의 기구에서 시행하는 "법독성학 전문가" 등 자격제도에 대한 인증이 이루어져 있다[86]. DFCB 또한 FSAB에 대한 자격제도 인증을 검토 중에 있다.

제6절 적격성 및 숙련도 시험

적격성 및 숙련도 시험(Competency and Proficiency Test)은 전문적인 능력의 보유 여부를 지속적으로 평가하기 위한 것으로 포렌식의 품질관리를 위해 매우 중요한 것이다.

숙련도 시험(proficiency test)은 랩 관리자나, 법 집행기관 혹은 포렌식랩에 의해 디지털 포렌식 검사관의 현재의 지식(knowledge), 기술(skills), 능력(abilities)를 평가하기 위한 것이며, 적격성(competency) 테스트는 일반적으로 디지털 포렌식 검사의 특별한 응용에서의 검사관의 지식, 기술, 능력을 평가하는 것이다. 예를 들어 훈련이 끝난 후에 관리자는 검사관이 그 훈련 내용을 마스터하고 배운 것을 실제 증거에 적용할 수 있는 지를 결정하기 위해 적격성 테스트를 부과할 수 있다. 숙련도 시험은 특정한 작업(task)에서의 검사관의 기술을 측정하고 검사관의 기술을 평가하고 또한 일상적인 관점에서 검사관의 기술 뿐 아니라 랩의 품질관리시스템 및 절차가 지속적으로 상태를 유지

86) Forensic Specialties Accreditation Board, Inc., (http://www.thefsab.org) 참조.

하는 것을 보증하기 위해 이루어진다. ASCLD/LAB의 경우에 모든 인증받은 랩은 매년 한번 외부기관이나 ASCLD/LAB에서 승인한 테스트 서비스 제공자에 의한 외부 숙련도 검사를 받을 것을 요건으로 하고 있다. 하지만 적격성 테스트에 대해서는 그러한 요구가 없다.

미국 남부플로리다 대학교의 National Center for Forensic Science(NCFS) 및 평생교육부와 연계한 Digital Forensic Quality Solutions(DFQS)사는 최초로 외부 Competency와 Proficiency test를 시행할 계획임을 발표하였다. 이는 ASCLD/LAB이 2007년 10월 컴퓨터 포렌식 숙련도 시험에 대해 승인을 함으로써 이루어지게 된 것이다.[87]

제7절 장비와 도구

장비와 도구(tools)는 디지털 포렌식에서 갖추어야 할 어떻게 보면 가장 현실적인 것들이다. 필요한 장비나 도구는 일일이 지목하기 어려울 정도로 다양하며 이미 수많은 제품들이 출시되어 있다. 물론 법집행기관에 가장 큰 문제점은 이러한 장비나 도구를 충분히 구매할 예산을 가지고 있지 못하다는 것이다.

경우에 따라서는 수많은 포렌식 제품 중에서도 특정한 범죄현장에서 필요한 기능을 보유하고 있지 않아 새로운 도구의 필요성이 제기되기도 한다. 이러한 수요에 감당하기 위해 일부 수사기관은 자체적인 개발부서를 두거나 개발업체에 의뢰하여 납품을 받기도 한다. 물론, 이러한 경우의 도구들은 잘 상용화되지는 않는다. 도구 자체가 비밀을 유지해야할 수사방법에 속할 수도 있기 때문이다. 수사기관은 제품을 자체적으로 개발할 수 있는 인적자원을 가지고 있거나 필요에 따라 이를 구매할 예산을 확보하는 것이 긴요하다고 하겠다. 일일이 필요한 장비와 도구의 목록을 작성하기는 어려울 것이다. FBI의 CART나 RCFL 등에서 대체적으로 어느 정도의 장비와 도구를 보유하고 있는 지는 이미 부분적으로 언급한 바 있다.

---

87) Digital Forensics Quality Solutions (http://www.ncfs.org/dfqs/index.html) 참조

하지만 필요한 도구를 보유하는 것만이 문제가 아니라 그 도구 자체가 신뢰성을 가지고 있는 검증된 도구여야 한다는 것은 이와는 구분되는 문제라고 할 수 있다. 도구의 신뢰성은 시험(test)을 거쳐 그 적격성이 확인되어야 하는데 구체적으로는 검증(validation)과 확인(verification)이 이루어져야 한다. validation은 시스템이나 컴포넌트의 개발 도중 혹은 마지막에 요구사항을 충족하는지는 판단하기 위해 평가하는 절차이며, verification은 주어진 개발 단계에서의 제품이 각 단계의 시작점에 주어진 조건을 만족하는지를 결정하기 위해 시스템이나 컴포넌트를 평가하는 과정이다.[88] 소프트웨어에 대해서는 IEEE standard 1012-1998과 IEEE draft P1012/D12 등의 기존의 시험 방법이 존재하지만 법과학적인 관점에서의 요구사항을 충족하는지는 별도로 확인될 필요가 있다.

이러한 필요에 의해 미 국립표준기술연구소(National Institute of Standards and Technology, NIST)는 국립사법연구소, 국방성 등의 지원을 받아 컴퓨터 포렌식 수사에 사용된 도구가 정확한 결과를 도출하는 지에 관한 보장여부를 측정하는 컴퓨터 포렌식 도구 검사(Computer Forensics Tool Testing, CFTT) 프로젝트를 진행하고 있다[89]. 이 프로젝트를 통해 제조업체는 품질을 향상시키고 수사기관과 같은 사용자들은 어떠한 제품을 선택할 지 결정할 때 도움을 받을 수 있으며 법조계에서는 각 도구의 기능성을 파악할 수 있다.

88) T. Wilsdon, J. Slay, "*Digital forensics: exploring validation, verification & certification*" Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on , vol., no., pp. 48-55, 7-9 Nov. 2005

89) http://www.ojp.usdoj.gov/nij/topics/ecrime/cftt.htm 참조

<표 15> 공개된 CFTT 검사 결과

도구 유형	제품명, 날짜
디지털 데이터 획득 도구	IXimager (Version 2.0, Feb-01 2006), April 2007
쓰기방지 장치	FastBloc FE (USB Interface), June 2007
	FastBloc FE (FireWire Interface), June 2007
	Tableau T5 Forensic IDE Bridge (USB Interface), June 2007
	Tableau T5 Forensic IDE Bridge (FireWire Interface), June 2007
	Tableau Forensic SATA Bridge T3u (USB Interface), January 2007
	Tableau Forensic SATA Bridge T3u (FireWire Interface), January 2007
	Tableau Forensic IDE Pocket Bridge T14 (FireWire Interface), January 2007
	WiebeTech Forensic SATADock (FireWire Interface), December 2006
	WiebeTech Forensic SATADock (USB Interface), December 2006
	WiebeTech Forensic ComboDock (USB Interface), May 2006
	Digital Intelligence UltraBlock SATA (FireWire Interface), May 2006
	WiebeTech Bus Powered Forensic ComboDock (FireWire Interface), May 2006
	WiebeTech Bus Powered Forensic ComboDock (USB Interface), May 2006
	WiebeTech Forensic ComboDock (FireWire Interface), May 2006
	FastBloc IDE (Firmware Version 16), April 2006
	Digital Intelligence Firefly 800 IDE (FireWire Interface), April 2006
	MyKey NoWrite (Firmware Version 1.05), April 2006
	ICS ImageMasster DriveLock IDE (Firmware Version 17), April 2006
	WiebeTech FireWire DriveDock Combo (FireWire Interface), April 2006
	Digital Intelligence UltraBlock SATA (USB Interface), April 2006
쓰기방지 소프트웨어	PDBLOCK Version 1.02 (PDF-LITE), June 2005
	PDBLOCK Version 2.00, June 2005
	PDBLOCK Version 2.01, June 2005
	RCMP HDL VO.4, August 2004
	RCMP HDL VO.5, August 2004
	RCMP HDL VO.7, August 2004
	RCMP HDL VO.8, February 2004
디스크 이미지 도구	dd Provided with FreeBSD 4.4, January 2004
	SafeBack 2.18, June 2003
	EnCase 3.20, June 2003
	Partial Results from Prototype Testing Efforts for Disk Imaging Tools: SafeBack 2.0, April 2003
	Red Hat Linux dd Version: 7.1 GNU fileutils 4.0.36, August 2002

출처: http://www.ojp.usdoj.gov/nij/topics/ecrime/cftt.htm, 2007. 10. 20. 현재

검사과정에서 예컨데 Red Hat Linux에서 low-level에서의 복사와 raw-data의 변환 등에 사용되는 'dd'프로그램이 일부 커널 버전에서 경우에 따라 디스크의 마지막 섹터

를 읽지 못하는 문제점을 발견하고 이에 대한 기술적 대안을 마련하기도 했다. 현재 CFTT에서 진행 중인 검사 분야는 Disk Imaging, Write block(Software, Hardware), 삭제된 파일 복구, 모바일 디바이스 등이다.

제8절 절 차

방법(method)과 절차(procedure)는 범죄현장에서 증거수집 및 처리, 분석, 보고의 각 과정에서 혹은 포렌식랩에서 검사과정에서 성공적인 디지털 포렌식 작업을 위한 매우 중요한 요소이다. 법정에서 가장 쉽게 공격받는 요소는 디지털 포렌식을 수행하거나 증언하는 사람의 자격(credential)과 방법론(methodology)의 문제이다. 그러므로 공식적으로 방법론을 문서화하고 엄격하게 이를 따르도록 규율할 수 있는 방안이 마련되어야 한다.[90]

많은 표준과 가이드라인, 매뉴얼 등이 이러한 절차적인 규정을 위해서 제안 혹은 채택되었다. 다음은 그 중에서 미국 정부기관에서 제시된 것들만 추린 것이다.

Best Practices for Seizing Electronic Evidence, Unites States Secret Service

Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors, NIJ Special Report, January 2007

Electronic Crime Scene Investigation: A Guide for First Responders, NIJ Guide, June 2001

Forensic Examination of Digital Evidence: A Guide for Law Enforcement, NIJ Special Report, April 2004

Investigations Involving the Internet and Computer Networks, NIJ Special Report, January 2007

---

90) H. Wolfe, *"Setting up and electronic evidence forensics laboratory"*, Computer & Security vol22, No8, Elsevier, (http://www.compseconline.com/hottopics/hottopic_Feb04/settingupaforensicsunit.pdf), 2003.

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations; Computer Crime and Intellectual Property Section, Criminal Division United States Department of Justice, July 2002

제9절 표준화

디지털 포렌식 분야의 문제점 중의 하나는 표준과 공식적인 방법론의 부족이며 이로 인해 다른 법과학 분야에 비해 미성숙하였으며 훈련과 자격과 인증제도의 부족함으로 이어졌다.[91] 즉, 이러한 표준에 대한 요구는 사람, 교육·훈련, 도구, 포렌식랩, 절차, 인증과 자격 등 전 분야에 걸친 것이라고 할 수 있다. 이미 각 부분에서 표준화 문제가 다루어졌기 때문에 여기에서 전체적인 표준화 문제를 별도로 논하지는 않지만 일부 표준화가 이루어졌다고 하더라도 완전히 정착되었다고 보기 힘들며 빠르게 변화하는 디지털 분야의 요구를 계속적으로 받아들여야 하는 문제 등이 여전히 남아 있다.

또한 표준화는 국제적으로 혹은 국가적으로 진행이 될 수 있는데, 디지털 포렌식 기술이 흔히 활용되는 사이버범죄의 경우 국제범죄적인 성격이 매우 강하기 때문에 국가표준보다는 국제표준을 지향하는 것이 필요하다고 하겠다. 이와 관련해서 중요한 이슈 중의 하나는 정보공유 언어의 표준화 문제라고 할 수 있다. 국제적으로 디지털 증거 등과 관련된 정보를 교환할 때 사용할 컴퓨팅 언어의 선택의 문제가 또한 제기될 수 있다. 정보를 공유하기 위해서는 표준적인 형식이 필요한 것이다.

형사사법 분야에서 정보공유를 위해 제시된 가장 큰 프로젝트는 미 법무부가 추진하고 있는 Global Justice XML Data Model(Global JXDM)이다.[92] 이와 연계하여 미 국립법과학연구소는 Digital Evidence Markup Language(DEML)를 개발하고 있다.[93] 이러한 정보공유 모델에 사용되는 확장성 생성 언어(Extensible Markup

91) M. Simon, J. Slay, "*Forensic Computing Training, Certification and Accreditation: An Australian Overview*", in IFIP International Federation for Information Processing, Volume 237, Fifth World Conference on Information Security Education, eds. Futcher, L., Dodge, R., (Boston: Springer), pp. 105 - 112.

92) http://www.it.ojp.gov/topic.jsp?topic_id=43 참조.

Language, XML)은 하이퍼텍스트 생성 언어(HTML) 기능을 확장할 목적으로 월드 와이드 웹 컨소시엄(WWW Consorsium)에서 표준화한 페이지 기술 언어이다. 이 기술을 사용하면 보이는 화면에 추가하여 구조화된 데이터의 전달도 가능하며 전자화된 문자와 그래픽, 오디오, 비디오 등 멀티미디어 데이터를 교환, 저장하고 응용, 처리할 수 있다. 미 국립법과학연구소의 DEML은 객체지향 개발언어로 통합모델링 언어(Unified Modeling Language, UML)을 사용하고 있다.

향후 이러한 표준화된 정보공유 방식은 사이버범죄수사 등의 국제공조에서 또한 매우 중요한 문제로 제기될 수 있는 것으로, 이와 관련된 사항에 대한 사전적 대비가 필요하다고 하겠다.

제10절 연 구

연구는 디지털 포렌식의 전영역에서 매우 중요한 문제라고 하겠다. 아직 정착되지 않은 디지털 포렌식의 법적, 기술적, 운영적 각 측면에서의 이슈들에 대한 연구과제는 매우 광범위한 것이다. 앞서 각 영역에서의 연구성과 일부가 제시되었고, 신기술에 대한 연구 흐름에 관해서는 별도의 장에서 언급할 것이다. 연구는 대학, 공공기관 및 부설 연구기관, 민간기관 등 다양한 곳에서 이루어질 수 있는데, 100개 이상의 대학 내의 디지털 포렌식 과정을 지니고 있고 디지털 포렌식 시장의 상당량을 점유하고 있으며 정부가 연구를 위해 막대한 자금을 투입하고 있는 미국의 경우 연구의 필요성에 대한 인식과 투자는 매우 높은 수준이라고 할 것이다.

제11절 정보공유

정보를 공유하는 것은 중복되는 노력을 감소시키고 관련 커뮤니티의 소속감을 향상 시키는 등 여러모로 긍정적인 작용을 한다. 필요한 공유정보를 판단하거나 정보공유를 위

93) http://www.ncfs.org/digital_evd.html#research 참조

한 정보시스템 기반의 구축이나 공유의 포맷을 정하는 문제 등 여러 문제가 제기될 수 있을 것이다. 일부 정보공유와 관련된 문제는 뒤에서 다시 다루어질 것이다.

정보공유와 관련하여 가장 대표적인 사례는 미국 국립소프트웨어 참조 라이브러리(National Software Reference Library, NSRL)이다. 디지털 증거 검사 중에는 방대한 양을 파일을 대상으로 키워드 검색 등에 많은 시간을 보내게 된다. 하지만 사실 이 중에 상당량의 파일은 이미 정상적인 상용프로그램의 일부분으로 잠재적으로 그 내용에 대한 인지가 이루어진 상태이므로 수사를 위해 일일이 그 내용을 검색하는 것은 불필요한 작업에 불과할 수 있다. 반면에 범죄에 사용될 가능성이 높은 프로그램 또한 실제로는 그 내용을 알고 있는 것과 다를 바 없으므로 이러한 잠재적 인지 상태에 있는 파일에 대한 해쉬값의 데이터베이스를 구축하고 이를 이용하여 실제 증거 검사시 이를 걸러낸다면 작업의 효율성을 매우 높일 수 있다.

이러한 아이디어를 바탕으로 NSRL은 국립사법연구소와 여러 법집행기관 및 NIST의 지원을 받아 상용 소프트웨어와 악의적으로 여겨질 수 있는 스테가노그라피 혹은 해킹 스크립트 등의 구성 파일에 대해 SHA-1, MD5 및 CRC32 값을 추출하여 배포하는 작업을 2001. 10월부터 분기별로 하고 있다. 2007년 6월에 배포된 버전은 4,300만 개 이상의 파일에 대한 참조데이터세트(Reference Data Set)을 포함하고 있다. 많은 포렌식 도구들이 RDS를 증거파일의 해쉬값과 비교하는 기능을 포함하고 있다[94].

앞서 설명한 Global JXML의 표준화는 정보공유에 관한 표준화 문제로 볼 수 있다. 또 하나의 표준화가 필요한 정보공유에 관한 문제 중의 하나는 법과학적 이미지 포맷(Image)[95]에 관한 문제이다. 국내에서도 표준적 디스크 이미지 포맷에 관해 연구[96]가 이루어진 바 있지만 여전히 디지털 증거가 이미지라고 하는 특수한 형태로 수집, 이동되

94) http://www.nsrl.nist.gov/index.html 참조.

95) 이미징(imaging, 혹은 bit-stream copy, forensic copy)은 매체에 저장된 데이터를 bit단위까지 정확하게 복제하는 것이다(Bill Nelson, et.al., “Computer Forensics and Investigations”, Tompson, 2004. p.48). 원본에 손상을 방지하면서 복제본(image)을 대상으로 조사를 하여 삭제된 파일이나 숨겨진 데이터 등 일반적인 파일 복사에서 발견할 수 없는 숨은 증거까지 찾아내고 증거의 진정성과 무결성을 확보하기 위해 매우 빈번하게 사용되는 증거수집의 한 과정으로 받아들여지고 있다.

96) 예컨데 이상수 등, “대용량 저장 매체를 고려한 디스크 이미지 포맷”, 제1회 안티포렌식 대응기술 워크샵, 한국정보보호학회/한국디지털포렌힉학회, 2007년 8월, 67-76.

는 경우가 많아 이 문제는 향후 원격에서의 증거수집이나 증거의 관리, 원격 분석 등 많은 점에서 문제의 소지가 될 개연성이 높다고 하겠다.

이와 관련하여 Digital Forensic Research Workshop(DFRWS)는 2005년 Common Digital Evidence Storage Format(CDESF) 워킹그룹을 결성하여 데이터 저장과 전송을 위한 표준 포맷을 개발하는 프로젝트를 진행한 바 있다. 하지만 2007년 8월 목표를 달성하기에 필요한 충분한 자원을 가지고 있지 못하다는 이유로 워킹그룹은 해산되었다.[97]

97) http://www.dfrws.org/CDESF/index.shtml 참조.

제5장 국내 디지털 포렌식 기반 현황

경찰에서 컴퓨터와 관련된 범죄에 대한 수사는 1995년 당시 경찰청 외사담당관실 내에 해커수사대를 창설하면서 본격적으로 시작되었다. 사이버범죄가 급격히 증가하면서 몇 차례의 조직변화 후에 2000년 현재의 사이버테러대응센터의 위상을 구축하게 되었다. 2004. 12월에는 국내에서 처음으로 사이버테러대응센터 내에 디지털포렌식센터를 설치하였다. 따라서 조직의 형태로는 사이버수사 조직 내에 독립적인 형태의 포렌식랩을 두고 있는 형태로 볼 수 있다.

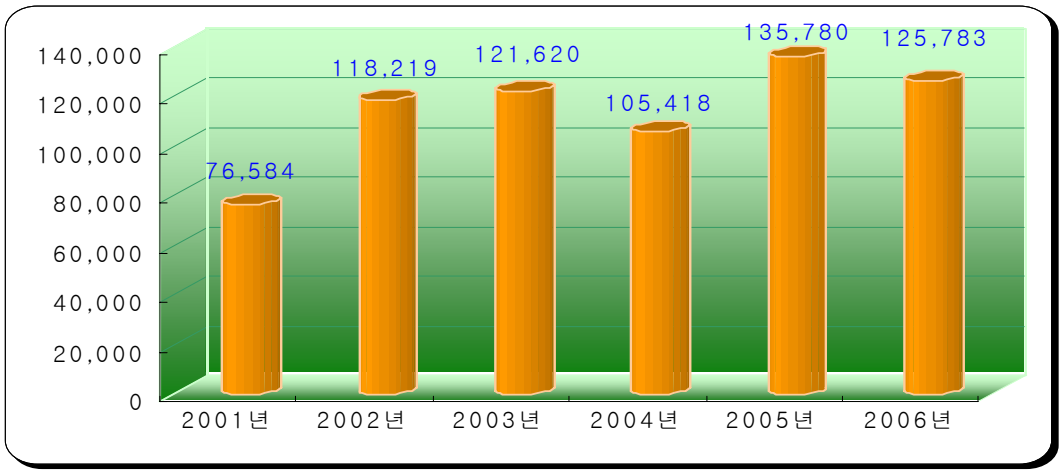
제1절 디지털 포렌식 수요 비교

1. 범죄사건의 양적 비교

현재 경찰의 디지털 포렌식 수요를 파악할 수 있는 체계적인 조사는 이루어진 적이 없는 것으로 보인다. 미국의 경우와도 범죄의 통계를 산출하는 방식이나 수사기관의 조직구조 등이 전혀 달라 이를 비교하기 쉽지 않다. 다만, 미국의 인터넷범죄신고센터와 경찰청 사이버테러대응센터에서 인터넷과 관련된 범죄를 관할에 관계없이 전국적 단일망으로 온라인 접수하고 있어 이 데이터가 양국의 사이버범죄 현황을 비교할 때 가장 신뢰성 있는 자료로 생각된다.

앞서 살펴본 바와 같이 미국에서 2006년도에 인터넷범죄신고센터를 통해 접수된 민원은 207,492 이다. 2006년도에 사이버테러대응센터에 온라인으로 신고된 민원은 모두 125,783건으로 미국의 60%정도에 이르고 있다. 이러한 숫자는 인터넷 사용자 수나 전체 범죄의 발생 건수 등 다른 통계와 비교하더라도 미국에 비해 상대적으로 국내 사이버범죄의 수가 매우 많다는 추론이 가능하게 하고, 결국 디지털 포렌식를 최대로 필요로 하는 범죄 형태 또한 사이버범죄라는 점, 국내에 IT 기술의 활용도가 매우 높은 점 등에

비추어 디지털 포렌식 수요 또한 최소한 인터넷을 통한 범죄 신고사건 비율인 60% 정도는 될 것으로 예측할 수 있다.



<그림 8> 경찰청 사이버테러대응센터의 인터넷민원(사이버범죄신고) 건수 (출처: 경찰청)

2. 디지털 포렌식의 인식에 기초한 비교

앞서 미국의 사례에서 본 바와 같이 디지털 포렌식에 대한 인식과 실제 범죄사건에서 디지털 증거의 포함여부는 매우 깊은 관계를 가지고 있다. 즉, 디지털 포렌식에 대한 경각심(awareness)이 높을수록 실제 범죄사건에서 디지털 증거를 포함하는 경우가 극적으로 높아지는 것이다.

또한 실제 디지털 증거가 활용되는 정확한 비중을 측정하려면 포렌식랩을 통한 디지털 증거의 분석량만을 비교해서는 안된다. 왜냐하면 미국의 경우 특히 연방수사기관의 경우 이제 디지털 포렌식의 중심이 포렌식랩으로 급격하게 전환이 되고 있지만 국내에서는 아직 포렌식랩이 활성화되었다고 보기 어려우며 많은 경우에 여전히 수사관들에 의해 디지털 증거의 수집 뿐 아니라 검사와 분석이 이루어지고 있기 때문이다.

실제로 디지털 포렌식에 대한 경찰의 인지도와 필요성에 대한 인식을 판단하기 위해 설문조사를 실시하였다. 설문조사의 내용과 분석결과는 부록으로 첨부하였다. 본 보고서

에서 이 조사가 차지하는 비중이 크지 않으며 실제 정확한 측정을 위해서 많은 변수들을 더 고려하여야 하고 면담 등 다른 조사방법이 병행되어야 할 것으로 생각되어 좀 더 광범위한 조사는 추후의 과제로 남겨두고 경감 기본교육을 받고 있는 경찰관 98명에 대해 설문을 실시하여 74명(76%)으로부터 응답을 받았다. 경감 계급은 경찰의 중간 관리자로 실무자에 대한 직접적인 감독책임을 지고 있기 때문에 설문의 대상으로 선정하였다. 설문 대상자 중에 사이버범죄수사에 전종하는 경우는 없었다.

설문 분석 결과 디지털 포렌식 자체에 대한 인지도는 매우 낮은 것으로 나타났다. 전체 응답자 중 '디지털 포렌식이 무엇을 하는 것인지 알고 있다'라는 질문에 그렇지 않은 편이다(27%), 전혀 그렇지 않다(20%)라는 답변이 전체의 47%였다. 경찰청 디지털포렌식센터의 존재에 대한 질문에 전체의 46%가 잘 모르거나 전혀 알지 못한다고 답변하였고, 디지털포렌식센터의 포렌식서비스에 대해서는 58%, 디지털 증거분석 의뢰 절차에 대해서는 73%, 디지털 증거처리 표준 가이드라인의 존재에 대해서는 82%, 이미징 기술에 대해서는 74%, 디지털 매체의 포장과 이송방법은 74%, 디지털 증거의 증거능력 문제는 66%가 잘 모르거나 전혀 알지 못한다고 답변하였다. 이러한 낮은 인지도는 연령이 높을수록 경찰청이나 지방경찰청 보다는 경찰서 이하에서 근무할수록, 범죄수사 부서가 전혀 포함되어 있지 않은 경무나 생활안전 분야에서 보다 높게 나타났다.

반면 디지털 포렌식의 수사상 필요에 대해서는 65%가 정말 그렇다 혹은 그런 편이라고 긍정적인 답변을 하였으며, 디지털 포렌식의 발전을 위해 가장 시급한 과제는 충분한 전문인력의 확보(52%), 교육 및 훈련(23%)의 순으로 나타났다. 디지털 포렌식의 발전에 대한 장애요소로는 인식부족(30%)과 예산부족(22%)이 가장 중요한 것으로 나타났으며, 가장 활용도가 높은 디지털 포렌식 기술로는 현장수사(43%)와 하드디스크 분석(35%)을 꼽았다.

실제 디지털 포렌식 기술의 활용빈도와 관련하여 수사경험이 있는 대상자 중에 별로 없다(37%), 전혀 없다(19%) 등 부정적 답변이 가끔 있다(22%), 매우 자주 있다(7%) 등 긍정적 답변보다 매우 높게 나타났다. 전문인력과 장비 등 필요한 자원의 보강에 대해서는 수사경험이 있는 응답자의 89%가 보강의 필요성을 느끼고 있는 것으로 나타났다.

결론적으로 디지털 포렌식에 대한 경찰 중간 관리자의 인지도와 필요성의 인식, 실제 활용도는 매우 낮은 편으로 볼 수 있는데, 그만큼 이 분야가 아직 경찰 내에서 중요한

수사방법 내지 증거획득 방법으로 인식이 되지 못하고 있는 것으로 보인다. 범죄사건과 증거의 속성 자체가 국가간에 매우 크다고는 보기 어렵기 때문에 미국의 경우, 특히 연방기관의 경우와 비교해보면 이 결과는 실제로 디지털 포렌식의 수요가 적다기 보다 디지털 포렌식의 수요가 있음에도 이를 인식하지 못하고 있다는 결과로 해석이 가능한 것으로 보인다.

제2절 법 률

1. 디지털 증거의 획득과 관련된 법률

미국의 사례에 비추어 국내의 형사소송법, 통신비밀보호법, 전기통신사업법 등 관련 법률에서 정한 규율의 구체성이 부족할 뿐 아니라, 컴퓨터 및 네트워크와 관련된 제반 범죄현상과 이를 수사하기 위한 방법상의 특성을 충분히 고려하지 못하고 있다고 볼 수 있다. 더욱이 2007년 형사소송법의 개정 전까지 물리적인 증거의 경우 위법수집 증거의 배제 법칙을 적용하지 않고 있었기 때문에 법정에서의 이를 둘러싼 논쟁과 그 결과물이라고 할 수 있는 판례가 충분히 축적되어 있지 않아 더더욱 판단의 준거가 부족한 상황이다.

때로 이러한 법적 규율의 부재는 정보가 아닌 하드웨어까지 광범위하게 압수를 허용하고 그 내용을 샅샅이 수색하여 '털어서 먼지 안나는 사람 없다'는 식으로 본래 사건과 관련이 없는 전혀 새로운 혐의를 발견하는 등 수사기관에 과도한 권한을 허용하는 결과가 되기도 하고, 특성상 본질적으로 필요한 해킹사건 수사를 위한 감청이 허용되지 않는다거나 로그기록의 보존명령 제도가 없는 등의 이유로 결과적으로 범죄자의 안식처를 제공하는 결과를 낳기도 한다. 수사권한이 남용되어 통신비밀과 프라이버시 등 헌법적 권한을 침해하는 문제도 심각하겠지만 적절한 법적 무기는 주지 않고 범죄에 대한 대응책임만이 수사기관에 주어지는 것도 큰 문제가 아닐 수 없다.

2. 증거능력과 관련된 문제

증거능력과 관련해서도 국내 법률은 무엇보다 규율 자체가 부재한 상황이다. 최근의 한 연구에서는 출력서면으로 전환되는 전자기록은 서증에 관한 현행규정 즉 전문법칙을 적용할 수 있지만 원본과 출력서면의 동일성을 입증할 수 있는 법적 기준이나 절차가 마련되어 있지 않고, 작성자나 진술자의 진술에 의한 진정성립의 증명이 어렵기 때문에 여전히 입증의 문제가 곤란을 겪고 있고, 그 기록이 기계적인 결과물에 지나지 않는 경우에는 비진술증거로서 전문증거에서 배제되어 실물증거가 되기 때문에, 이러한 경우에는 적절하고 합리적인 진정성 입증절차를 거쳐 그 증거능력을 허용하는 것이 합리적이라 할 수 있는데, 우리 법원에서는 아직 이러한 디지털 증거의 증거능력에 대한 판단이나 해석이 나오지 않고 있어 결국 디지털 증거 자체에 의한 사실인정은 현실적으로 불가능한 일이라고까지 하고 있다.[98]

디지털 포렌식에서 취급하는 증거들은 기존의 증거에 관한 규칙들을 그대로 적용할 것인지 판단하기 어렵게 하는 특징들을 지니고 있기 때문에 실무가들의 어려움은 가중될 수밖에 없다. 따라서 우선적으로 디지털 증거의 취급에 관한 가능한 범위 내에서의 입법적인 해결책이 제시되어야 한다는 주장[99]은 타당한 지적이라고 할 수 있다.

최근 항소심[100]에서 전문증거의 진정성 확인 절차가 포함되지 않아 파기되기는 했지만 일정한 요건을 충족하는 경우 디지털 증거의 증거능력을 인정하는 내용을 포함하는 전향적 하급심 판결[101]이 있었던 것으로 보아 향후 법원의 디지털 증거를 보는 시각의 변화를 기대하게 하고 있다.[102]

한편 증거의 신빙성 문제에서 중요한 내용이 될 과학적 증거의 인정 여부에 대해서도 한국의 입법이나 판례상 과학적 증거의 허용성에 대한 일반적 지침이 아직 확립되어 있지 않고 어떠한 분야에 대해서는 너무 엄격하게 반대로 다른 분야는 너무 느슨한 기준을

98) 탁희성, “법정에서 디지털 증거의 허용가능성”, 디지털포렌식연구 창간호 23-41, 2007. 11, 25-27면.
99) 예컨데 양근원, 형사절차상 디지털 증거의 수집과 증거능력에 관한 연구, 경희대학교 박사학위 논문, 2006, 591면.
100) 서울고등법원 형사3부 2007. 8. 16. 선고. (일명 일심회 판결)
101) 서울중앙지방법원 2007. 4. 16. 선고 2006고합 1365.
102) 탁희성, 전게 논문, 27-28면.

적용하고 있다는 비판이 있다.[103] 이에 대해서도 법원의 태도에 큰 변화가 없었으나 최근 대법원이 DNA 검사결과가 문제된 사건에서 '과학적 증거방법은 그 전제로 하는 사실이 모두 진실임이 입증되고 그 추론의 방법이 과학적으로 정당하여 오류의 가능성이 전무하거나 무시할 정도로 극소한 것으로 인정되는 경우에는 법관이 사실인정을 함에 있어 상당한 정도로 구속력을 가진다.'고 판시[104]하여 과학적 증거에 대한 합리적인 인정기준의 제시에 대한 기대를 해볼 수 있을 것으로 보인다.

하지만 지금까지 법률적인 적절한 통제의 부재상황은 디지털 포렌식의 전반적인 발전에 매우 부정적인 영향을 미친 것으로 생각된다. 미국의 경우를 보더라도 법적인 요구들이 인증제도, 표준절차, 자격제도 등 많은 기반제도들의 발달하게 한 주요한 요인이 되었는데 법적인 요구가 분명하지 않은 상황에서 스스로를 까다롭고 엄격하게 통제할 것을 기대하는 것은 아무래도 일정한 한계가 있기 때문이다.

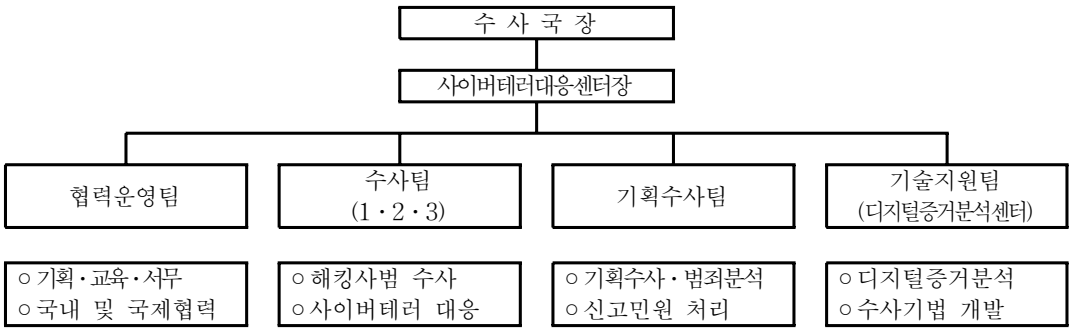
제3절 조직 운영

1. 조직과 인력

경찰의 디지털 포렌식 조직은 <표 16>과 같이 경찰청 수사국 소속에 사이버테러대응센터와 그 하부조직으로 디지털 포렌식 센터를 두고 있다. 경찰청 사무분장 규칙 (일부개정 2007. 7. 2 개정, 경찰청 훈령 제508호)에서 기술지원팀(디지털증거분석센터)이 담당하는 기법개발업무는 ①사이버테러 예방전략 연구 및 개발, ②사이버범죄 관련 보안·수사기법 연구, ③사이버수사 기술 지원, ④디지털 증거분석 업무 등을 담당하는 것으로 정해져 있다. 즉, 연구·개발(R&D)와 디지털증거분석 실무를 병행하고 있는 것이다.

103) 심희기, "과학적 증거의 허용성과 신빙성", 고시계 제514호 5-15, 1999. 11, 15면.
104) 대법원 2007. 5. 10. 선고 2007도1950.

<표 16> 경찰청 사이버테러대응센터 조직



디지털 포렌식 센터에는 10여명의 계약직 포함 일반직 공무원과 소수의 경찰공무원이 R&D와 증거분석 업무를 병행하고 있는 것으로 알려져 있다. 현재 경찰에는 경찰청 사이버테러대응센터 외에 지방경찰청의 사이버범죄수사대, 각 경찰서에 사이버범죄수사팀 혹은 '반'규모로 전국적으로 900명에 가까운 사이버수사요원이 근무하고 있으며, 이중에 160여 명은 컴퓨터 관련 전공자로 특별채용된 인원이다. 이중에 실제 디지털 증거분석에 관여하는 인력 및 관련 기반의 현황은 <표 17>과 같다.

<표 17> 경찰의 디지털증거분석실 및 분석인력 현황 (자료: 경찰청)

연번	지방청	인력운영		증거분석 실적							
		인력	IT 전공	총계		'05		'06		07. 1-4'	
				건수	매체	건수	매체	건수	매체	건수	매체
총계		45	33	936	2,748	122	274	546	1,787	268	687
0	경찰청	16	9	220	543	80	174	98	253	42	116
1	서울	5	4	133	441	12	20	83	334	38	87
2	부산	3	2	77	522	0	0	49	430	28	92
3	대구	2	2	19	26	0	0	13	16	6	10
4	인천	2	2	39	67	0	0	29	51	10	16
5	울산	1	1	26	67	1	2	23	41	2	24
6	경기	2	2	66	164	12	14	34	76	20	74
7	강원	1	1	28	139	0	0	15	84	13	55
8	충북	2	2	34	57	2	6	15	30	17	21
9	충남	2	2	153	413	8	44	97	279	48	90
10	전북	2	1	35	82	5	11	20	57	10	14
11	전남	2	0	48	98	2	3	36	63	10	32
12	경북	2	2	25	80	0	0	17	40	8	40
13	경남	2	2	25	40	0	0	13	28	12	12
14	제주	1	1	8	9	0	0	4	5	4	4

조직구성과 관련하여 발견되는 문제점은 무엇보다 수사관과 증거분석을 담당하는 디지털 포렌식 검사관 등에 대한 명확한 구분이 없다는 점, 법과학의 중심적 요소 중의 하나인 포렌식랩의 기반이 완전히 구축되지 않았다는 점, 가능한 포렌식서비스에 대한 공개된 문서가 없다는 점, 범죄현장에서 압수수색 등 지원업무가 명확한 포렌식서비스로 명시되어 있지 않다는 점 등 여러가지를 들 수 있다.

2. 디지털 증거분석량

아직 경찰에서 디지털증거분석 현황에 대한 정밀한 통계를 작성하지 않고 있으나, 특히 지방청 단위에서 디지털증거분석이 활성화되기 시작한 2005년 이후의 통계를 보더라도 2005년에 122건 274개 매체에 대한 분석이 이루어졌으나 2006년에는 546건 1,787개 매체로, 2007년 4월까지 268건에 687건의 매체로 디지털 증거분석은 급격한 증가추세를 보이고 있다.

하지만 증거분석인력은 전체 38명에 불과하고 그나마 이중 22명만이 증거분석 업무에 전종하고 16명은 수사업무를 병행하고 있어 사이버범죄만도 연간 8만 건 이상을 처리하는 경찰의 실정에 비추어 분석요원의 심각한 부족현상이 예측된다.

게다가 2006년의 경우 행정직 포함 22명이 근무하는 미국 San Diego RCFL에서 분석된 매체건수가 5,138개임을 고려할 때 분석량 자체가 1,787개 매체에 불과한 것은 연간 사이버범죄만도 8만 건 이상을 수사하는 경찰의 상황에 비추어 매우 저조한 상황으로 생각된다. 그 원인으로는 무엇보다 아직 디지털 증거 수집의 필요성을 인식하지 못하고 있거나, 아니면 수사업무를 병행하면서 많은 수사관들이 여전히 스스로 담당 사건에 대한 증거수집을 하기 때문인 것으로 보인다.

좀 더 구체적인 현황파악을 위해 3개 지방경찰청 사이버범죄수사대에서 2006년 이후 2007년 10월까지 작성된 111건의 증거분석 결과를 제공받아 분석해 그 결과를 <표 18> 3개 지방경찰청 증거분석 표본분석으로 정리하였다.

<표 18> 3개 지방경찰청 증거분석 표본분석

조사항목	결 과	비 고
사건수	111건 자체: 24건 타부서 의뢰: 87건	※3개 지방청 분석요원 7명 전종 2명, 수사겸직 5명
매체수	전체 375개 사건별 평균 3.07개	시스템 의뢰 198대 (분석된 HDD 194개) HDD만 의뢰 144개 flash memory 1개 DVD 1개, 파일로 제출 35건
평균 매체용량	2006년 평균 68.33GB 2007년 평균 89.14GB	2006년 전체 추산 119.24TB(1,787*68.33/1,024)
평균 분석 소요 시간 (일수로 계산)	분석시간이 확인된 99건 중 사건별 10.01일 매체별 3.24일	

3개 지방청에서 증거분석보고서가 작성된 사건은 모두 111건, 매체수로는 375개로, 이중에서 지방경찰청 사이버범죄수사대에서 수사 중인 사건에 대한 분석이 24건(21.6%), 지방경찰청의 타부서나 경찰서에서 의뢰된 사건이 87건(78.3%)이다. 그 중 증거분석을 의뢰할 때는 PC나 노트북, 서버 등 시스템 자체를 제출하여 의뢰한 경우가 198건이나 되고 있고 특히 이미지를 제출한 경우한 경우는 한 건도 없어 아직 일반화된 증거분석 절차조차 일상화되고 있지 않음을 보여준다.

증거분석 의뢰 매체의 경우 시스템 자체를 의뢰(198대)하거나 HDD(하드디스크 드라이브)를 제출하여 하드디스크를 분석 대상으로 한 경우가 90.1%에 달하고 flash memory와 dvd의 경우 각 1건에 불과하며 파일만을 제출한 경우가 35건에 이르고 있었다. 이는 미국 RCFL의 증거분석의 경우 2006년 CD가 20,960건, 플로피 디스크가 16,019건, HDD가 15,079건이며 PDA, Tape 등 다른 다양한 매체가 분석되고 있는 것에 비해 차이가 있다.

개별 매체의 평균적인 용량은 2006년 68.33GB에서 2007년에 89.14GB로 증가하였으며 이를 경찰청에서 집계한 2006년 중 전체 디지털 증거분석 매체분량 1,787개에 대해 적용하면 대략적으로 2006년도 경찰에서 디지털 증거분석이 된 대상 매체들의 총

용량은 119TB 가량으로 추산할 수 있다. 이 또한 미국의 RCFL이나 CART의 통계치에 비추어 매우 적은 양이라고 볼 수 있다.

앞서 디지털 포렌식에 대한 인식이 실제 디지털 포렌식의 활용에 미치는 영향이 크다는 미국의 연구결과를 소개하고 다시 설문조사를 통해 국내 경찰관의 디지털 포렌식에 대한 인식이 높지 않다는 사실을 확인하였는바, 위와 같은 디지털 포렌식 분석에 대한 실적 분석은 앞선 연구에서 추론할 수 있는 바와 일치하는 것이다.

3. 예 산

경찰청 사이버테러대응센터의 예산현황은 <표 19>와 같으나, 실제 동 예산 중 디지털 포렌식에 사용되는 순수 예산이 얼마인지는 알기 어렵다고 하더라도 미국의 RCFL 등의 예산과 비교해서 턱없이 부족하다는 사실은 쉽게 알 수 있다.

<표 19> 경찰청 사이버테러대응센터 예산 배정 현황 (단위: 억원)

구 분	합 계	운영비	국제여비	용역비	시설비	유형자산
2005	24.4	10.8	0.2	1.4	-	12.0
2006	29.4	11.5	0.5	1.4	-	16.0
2007	27.9	11.2	0.6	3.0	-	13.1
2008(안)	29.4	12.2	0.6	3.0	1.2	12.4

제4절 교육·훈련 및 자격제도

1. 경찰에서 자체 운영하는 과정

경찰에서 자체적으로 디지털 포렌식에 특화하여 실시하는 교육은 공식적으로는 경찰수사연수원의 디지털증거분석 프로그램 전문과정이 유일하다. 이 교육은 한회에 1주일, 40명씩 연간 2회 80명의 사이버수사요원 특별채용자와 사이버수사 2년 이상 경력자에

대해서 디지털 증거분석 등 6개 과목에 대해서 실시되고 있다.

<표 20> 수사연수원 디지털증거분석전문과정 교과(소양과목 제외)

과 목 명	시 간
디지털 증거분석 개요	2
증거분석절차 및 툴 소개	4
휘발성 증거 수집 분석	4
비휘발성 증거 수집 분석	4
증거분석 프로그램 실습	14
증거능력관련 형소법 연구	3
합 계	**31**

(출처: 경찰수사연수원 http://www.kpia.go.kr)

2. 경찰에서 실시하는 민간위탁교육(훈련)

경찰에서 2007년 중 디지털 포렌식과 관련하여 민간 교육기관에 의뢰하여 실시하는 교육현황은 <표 21>와 같다.

<표 21> 사이버범죄 관련 민간위탁교육(2007, 계획) (자료: 경찰청)

구 분	과정명	일 정	인 원
총 계			100명
사이버범죄 수사과정	해킹・악성코드분석	3주	23
	인터넷추적	5일	16
디지털증거분석과정	데이터베이스	5일	43
	Encase 고급과정	4일	16
	디지털증거 물리복구	5일	2

3. 일반 전문교육(훈련)

디지털 포렌식과 관련된 공개된 훈련 프로그램은 거의 전무한 것이나 다름이 없는 실정이다. 특정기술이나 제품과 관련된 위의 몇몇 과정을 제외하면 한국생산성본부와 사단법인 사이버포렌식협회에서 실시하는 사이버포렌식전문가 프로그램이 거의 유일한 것이다. 이 프로그램은 한국생산성본부의 민간자격인 사이버포렌식전문가 자격프로그램과 연계되어 있다.

<표 22> 한국생산성본부 사이버포렌식조사전문가 과정 커리큘럼

모 듈 명	강 좌 명	내 용
사이버포렌식 특강 (18시간)	기업기밀보호(3시간)	기업 정보보호 산업 기밀보호와 산업스파이
	사이버법률 1(15시간)	법률과 포렌식(형법,형소법,증거법 등)
포렌식 기술 (36시간)	범죄심리학(3시간)	사이버범죄 심리학
	사이버포렌식 총론(3시간)	포렌식 총론 포렌식 개요와 추세, 발전방향
	디스크 포렌식(12시간)	윈도우즈시스템 포렌식 윈도우 파일 복구 (실습,플로피,USB 등)
	DB포렌식 및 포렌식 실무(12시간)	데이터베이스 포렌식 포렌식 실무
조사실무 (24시간)	네트웍/시스템(6시간)	네트워크/시스템상 증거수집과 분석
	안티포렌식(3시간)	안티포렌식 동향과 추세
	포렌식 조사 개론(12시간)	포렌식 조사관의 자세와 조사 기법 조사보고서 작성절차와 방법
	포렌식 조사/실습(12시간)	사례별 조사보고서 작성요령 및 실습 등

(출처: 한국생산성본부 http://www.kpc.or.kr)

4. 대학교육

국내 대학교육에서 모든 종류의 법과학 분야에 대한 관심은 매우 저조한 상황이다. 법과학과 관련된 학부의 전공과정은 거의 전무하며, 석사과정 또한 일부 의과대학의 법의학과정과 다소 포괄적인 의미에서 과학수사전공 등의 석사과정이 몇몇 대학원에 개설되어 있으나 다수의 분야별 석·학사 과정이 개설되어 있는 미국이나 영국 등 법과학 선진국과는 비교하기 어려운 수준이라고 볼 수 있다.[105] 신생분야인 디지털 포렌식 분야에 대한 상황도 별로 다르지는 않은데, 고려대학교 정보경영공학 전문대학원(구 정보보호대학원)이 정보보호기술센터 내에 컴퓨터 포렌식연구실을 설치하여 국내에서는 가장 활발한 연구실적으로 보이고 있고, 포렌식 기술과 법률 등 수 개의 강좌를 개설한 것과 동국대학교, 전남대학교 등 몇몇 대학원의 정보보호 관련 학과에서 디지털 포렌식 연구를 병행하고 있는 것이 거의 전부라고 할 수 있다.

제5절 자격 및 인증제도

디지털포렌식에 특화된 자격으로는 공적자격으로 경찰청에서 2005년부터 시행하고 있는 전문수사관(디지털증거분석분야) 제도와 민간자격으로 한국생산성본부의 사이버포렌식전문가가 있으나 앞서 미국의 경우에서 살펴본 것과 같이 디지털포렌식 실무가가 갖추어야 할 최소한의 지식, 기술, 능력이 무엇인지에 대한 관련 커뮤니티의 합의 등 판단 준거가 없는 상황이고, 미국의 법집행기관의 자체 인증과정이나 국립법과학센터의 새로운 국가적 자격제도안의 커리큘럼 등에 비추어 교육생의 요건이나 교육시간 등 전반적인 측면에서 필요충분한 자격제도의 요건을 갖추었다고 보기 어렵다.

한편으로는 아직 국내에서 디지털 포렌식에 대한 연구와 실무의 역사가 일천하여 체계적인 기반의 구축과 자질이 보증된 강사의 확보, 교육장 시설, 훈련 프로그램 개발 등에서 일정 수준 이상의 훈련 프로그램을 운영할 기반이 취약한 상태이므로 자격제도 자체

105) 법과학 관련 교육 현황에 대해 상세한 것은 임준태, 과학수사기반 구축을 위한 법과학교육 활성화, 한국경찰학회보, Vol 14, 3-42, 2007. 참조

를 바로 마련할 것이 아니라 이러한 기반을 속히 구축하는 것이 우선되어야 할 것이다.

이 교육 자체에 대한 인증은 물론 포렌식랩에 대한 인증 사례도 아직 없을 뿐 아니라, 인증제도가 포렌식의 품질을 보증하는 매우 중요한 요소라는 사실에 대한 사회적 인지가 아직 이루어져 있지 않은 것으로 보인다.

제6절 전문가 공동체

미국에서 많은 디지털 포렌식의 발전이 정부기관의 지원을 받는 워킹그룹이나 협회, 법과학 단체 등 전문가 커뮤니티의 노력에 의해 이루어졌음은 앞에서 살펴본 바와 같다. 국내에 이러한 형태의 커뮤니티는 거의 전무한 상태에서 2005년 많은 관계기관, 학계의 전문가들이 모인 한국 디지털포렌식학회가 창설되어 각종 세미나, 워크샵, 학회지 발간 등 활발하게 활동을 하고 있어 그 역할이 주목되고 있다.

하지만 이러한 변화에도 불구하고 미국의 경우처럼 디지털 포렌식 공동체에서 주요한 역할을 해야할 수사기관 및 관련 정부기관간의 협력은 그다지 활발하지 못한 것으로 보인다. 이러한 문제가 비단 디지털포렌식만의 문제라고는 볼 수 없지만 이 분야의 발전에 앞장 서야할 기관들이 뜻을 같이 하기 어렵다는 것은 참으로 아쉬운 일이 아닐 수 없다.

제7절 기 타

표준화와 관련하여 경찰청과 한국디지털포렌식학회는 2006년말 공동으로 디지털 증거처리 표준 가이드라인을 제정한바 있다. 이외에도 한국전자통신연구원(ETRI)는 경찰청과 한국디지털포렌식학회의 '디지털증거처리 표준 가이드라인' 등을 고려하여 미국의 CFTT와 유사한 증거수집 및 분석도구 검증절차 표준화 등을 추진하고 있는 것으로 알려져 있다. 하지만 이미 여러 학술회의 등에서 여러 측면에서 표준화의 필요성이 제기되었음에도 불구하고 실제로 표준화가 이루어지는 속도는 매우 느린 상태라고 할 수 있다.

특히 많은 표준화 작업들이 국제표준이나 미국표준 등 영어로 표현된 표준안을 기준으로 작성되는 것이 현실인 상황에서 용어의 표준화와 같은 기초작업에 대한 필요성이 크다. 디지털 포렌식 작업을 통해 작성된 문서는 흔히 비전문가들에게 제공되므로 전문적인 용어보다는 일반적인 용어로 작성될 것이 권장되며 필수적으로 사용되는 전문적인 용어는 그 의미를 포렌식 보고서의 초반 부에 별도로 기재하는 것이 외국의 포렌식 보고서 작성의 일반적인 방식이다. 국내에서는 1995년부터 정보통신부, 문화관광부, 기술표준원 등 3개 기관이 공동으로 정보통신용어표준화 사업을 진행하여 2006년 12월 기준으로 23,000여 개의 용어가 표준용어로 채택되어 CD-Rom과 웹을 통해서 제공되고 있다.[106]

하지만 슬랙스페이스(slace space), 법과학적 복제 혹은 이미징(imaging)과 같이 포렌식에서 흔히 사용되는 용어는 표준용어에 포함되어 있지 않고 한글화하여 표시하기가 쉽지 않으며 실무적으로 통일적으로 사용되고 있지도 않다. 따라서 이러한 용어의 표준을 정할 필요가 매우 크다.

이 작업을 통해 외국의 경우처럼 포렌식 보고서에 용례(glossary)를 기재하기 보다는 표준화된 용어집을 활용하여 보고서 작성자나 이를 읽는 사람이나 그 정확한 의미를 공유할 수 있는 방안을 활용하는 것이 크게 효율화될 수 있을 것이다.

106) http://word.tta.or.kr 참조

제6장 신기술의 연구·개발 문제

연구·개발(R&D)은 디지털 포렌식과 범죄수사에 다양한 형태로 발생하고 있는 기술적인 난제들을 해결함과 동시에 법적, 운영적인 요구사항을 수용하는데 매우 중요한 요소임에 틀림이 없다. 기존의 기술이 발달했다고는 하지만 여전히 새로이 개발되어야 할 기술과 도구는 일일이 열거하기 힘들 정도로 많다고 할 것이다. 오늘날까지 컴퓨터 포렌식은 주로 명확한 이론적 기반에 대한 고려가 거의 없는 업체와 응용기술에 의해 주도되어 왔다.[107] 따라서 여기에서는 이러한 연구·개발에 있어 향후 방향성을 제시하는 수준에서 고려되어야할 일부 분야를 중심으로 살펴보도록 하겠다.

제1절 신기술 개발 수요 분석 사례

2001년부터 2003년까지 미국 다츠머스 대학의 보안공학연구소(Institute for Security Technology Studies, ISTS)는 디지털 증거의 수집을 포함하여 사이버공격에 대한 수사에 필요한 도구와 기술의 수요와 현황을 파악하고 연구·개발의 우선과제를 선정하기 위한 '사이버공격에 대한 수사를 위한 법집행 도구와 기술'이라는 대규모 연구를 수행하였다. 그 결과는 '국가적 수요 측정'[108], '격차 분석 보고'[109]를 거쳐 최종적으로 2004년 '국가 연구 및 개발 과제'[110]라는 주제로 각각 발표되었다. 이 보고서에 나타

107) B. Carrier and E. Spafford. "*Getting physical with the digital forensics investigation*", International Journal of Digital Evidence 2003:2(2).

108) Institute for Security Technology Studies, "*Law Enforcement Tools and Technologies for Investigating Cyber Attacks*", (http://www.ists.dartmouth.edu/TAG/needs/ISTS_NA.pdf), 2002.

109) Institute for Security Technology Studies, "*Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report*", (http://www.ists.dartmouth.edu/TAG/gar/ISTSGapAnalysis2004.pdf), 2004.

110) Institute for Security Technology Studies, "*Law Enforcement Tools and Technologies*

난 주요 연구·개발 수요는 디지털 포렌식의 기술과 도구 개발 연구 과제에 대부분 포함될 수 있는 것들로 이를 정리하면 아래와 같다. 한편 최종 보고서에서는 수년간에 걸친 연구기간 동안 기술과 도구에 대한 수요에 따른 연구·개발이 있을 것으로 기대했지만 그 수요가 그대로 존재하고 있었다고 결론짓고 있다. 이러한 상황은 지금까지도 크게 변동이 없는 것으로 생각된다.

1. 수사 과정 : 예비 조사와 데이터 수집

○ 다중의 운영체제 시스템으로부터 데이터 수집을 자동화하는 솔루션

이미 상당수의 제품이 출시되어 있지만 값이 비싸고 법집행에 특화된 기능이 부족하다

○ 네트워크 매핑과 결과물의 그래픽으로의 산출

특히 내부자가 용의자인 경우가 많은 사이버공격에 대한 수사의 특성상, 내부자의 도움이 없이 속칭 네트워크 구성도라고 불리는 네트워크 맵(network map)에 대한 자동화된 그리고 그래픽으로 쉽게 알 수 있는 결과물을 보여주는 솔루션에 대한 수요가 크다

○ 플랫폼이나 포맷과 관계없는 로그의 검색, 인지, 수집 솔루션

다양한 운영체제 혹은 응용프로그램의 로그들을 플랫폼이나 포맷과 관계없이 자동으로 인지하고 수집해주는 솔루션

○ 메모리의 데이터 수집 솔루션

살아 있는 컴퓨터의 메모리에 들어 있는 데이터를 수집해주는 솔루션

---

for Investigating Cyber Attacks: National Research and Development Agenda" http://www.ists.dartmouth.edu/TAG/agenda/ISTS_NRDA0604.pdf, 2004.

○ 매우 큰 데이터 집합에 대한 분석도구

매우 빠르게 증가하고 있는 저장장치 용량과 네트워크를 통한 많은 저장장치에의 접근을 필요로 하는 사이버공격의 특성을 고려한 대규모 데이터를 적절한 시간 내에 처리할 수 있는 도구

2. 수사 과정 : 로그 분석

○ 플랫폼이나 포맷과 관계없이 대량의 로그를 검색, 수집, 편집할 수 있는 솔루션

○ 또한 그 상세한 기술적인 정보를 그래픽 형태로 출력해주는 솔루션

3. 수사 과정: IP 추적과 실시간 감청

○ IP 스푸핑을 탐지, 추적, 대응할 수 있는 도구, 이에 대해서는 새로운 과학적 접근이 필요하다.

○ 관계없는 사람들의 프라이버시를 보호하면서 네트워크 감시과정에서 필요로 하는 데이터를 빠르고 정확하게, 또한 빠짐없이 추출하여 분리하고 분석할 수 있는 도구

4. 연구와 개발을 필요로 하는 신흥 기술

○ 암호해독 기술

암호는 이 분야의 수사에서 가장 큰 관심을 받고 있는 분야 중의 하나이다. 암호는 많은 운영체제와 응용프로그램에서 사용되어 매우 사용하기 쉽다. 관계자의 진술에 의하거나 다른 곳에 기재된 비밀번호를 발견하거나 키스트로그 로거(keystroke logger)에 의해 비밀번호를 알아내는 방법들을 흔히 사용하였지만 이러한 방법들은 많은 경우에 통용

이 되지 않는다. 복호화나 비밀번호 색출, 또 다른 단서의 발견 등 어떠한 방법이 되었던 간에 암호의 문제를 해결할 수 있는 새로운 과학적인 시도들이 필요하다

○ 디지털 스테가노그라피

데이터를 숨기는 기술인 스테가노그라피 또한 사용하기 쉽지만 그 기술이 사용되었는지를 인지하는 것조차 쉽지 않다. 이에 대한 연구가 진행되고 있지만 수사상 목적에 활용될 수 있기 위해 새로운 도구를 개발할 필요성이 크다.

5. 국가적인 정보의 공유

공격 패턴을 식별하기 위한 기술적 익스플로잇 매칭 솔루션과 연계된 공격 프로파일 수집을 위한 데이터 베이스

사이버공격의 특성상 많은 수사관은 같은 공격자에 의한 사건을 수사하게 되므로 이를 서로 비교분석할 수 있는 방법을 필요로 한다.

수사관들은 자신이 수사하고 있는 사건이 거대한 공격의 일부분인지 파악할 수 있게 하기 위해 공격 시그니처 데이터베이스로 역할을 하는 도구를 필요로 한다. 흔히 이러한 데이터베이스는 관할과 관계없이 커뮤니케이션이 가능한 것이 되어야 한다.

제2절 디지털포렌식 아키텍쳐와 Virtual LAB

1. 문제제기

전통적인 포렌식렙은 독립되고 폐쇄적인 공간을 활용하는 것이 일반적이다. 증거는 현장에서 수집되어 안전하게 포장된 후 포렌식랩으로 운반된다. 이러한 증거의 처리방식은 기존의 물리적인 증거를 취급하는 것과 특별히 다를 바가 없다.

증거의 발견과 수집, 이송과 검사, 분석과 결과의 제출과 같은 각 과정은 각각 자격

있는 '사람'에 의해 이루어진다. 하지만 실제로 디지털 증거를 이러한 물리적이며 사람에 의해 특정한 공간에서 이루어지는 것으로 취급하는 것은 뚜렷한 한계를 가지고 있다. 디지털 증거는 더 많은 곳에서 더 빠르게 수집되어야 하며, 많은 경우 사람이 아닌 신뢰성 있는 도구와 장비에 의해 진정성과 무결성이 확인될 수 있다. 결국 전통적인 현장과 단일한 포렌식랩이라고 하는 지리적 공간의 개념은 더 이상 유효하지 않을 수 있다. 하지만 이러한 문제는 포렌식랩의 인증과 같은 전통적인 법과학의 토대 위에 만들어진 여러 제도들을 혼란에 빠지게 할 수 있는 매우 중대한 문제라고 할 수 있다.

이에 따라 기존의 전통적인 법과학의 지리적 공간의 개념을 중심으로 한 포렌식을 사이버공간에서 존재하는 디지털 증거의 흐름에 주안점을 두되, 종래의 법과학적 제도의 다차원적인 측면을 그 개념안에 포섭하여 새로운 정보기술 아키텍쳐 기반(Information Technology Architecture based)의 디지털 포렌식의 도입과 같은 것을 검토할 필요가 있다.

2. 정보기술 아키텍쳐 기반의 포렌식 체계

복잡한 현실에서의 문제를 가시화, 표준화, 체계화하는 것으로 정보기술 아키텍처는 효율적인 정보시스템의 구축을 지원한다[111]. 유비쿼터스 환경에서 수집될 다양하고 방대한 디지털 증거의 처리를 위해 디지털 포렌식은 좀 더 인간보다는 정보와 컴퓨터, 네트워크 중심을 지향하게 될 것이다. 현장의 범죄감식 요원이 물리적인 증거를 수집하는 것에서 정보수집 기능을 가진 에이전트 프로그램이 미리 정해놓은 규칙에 따라 자동적으로 범죄와 관련된 증거자료를 수집하여 네트워크를 통해 중앙 저장장치에 전송하는 것으로 변화하는 형태가 단적인 사례가 될 것이다. 따라서 전체적인 의미에서의 디지털 포렌식 체계는 정보기술 아키텍처를 기반으로 할 필요가 있다.

정보기술 아키텍처는 전사적 정보구조(Enterprise Architecture), 기술참조모델(Reference Model), 표준프로파일(Standard Profile)라는 구성요소를 가지고 있다. 전사적 정보구조는 업무 및 관리 프로세스와 정보기술 간의 관계를 표현한 것이다. 정보,

111) 신신애, "EA(Enterprise Architecture)기반 표준화 추진 방안", 정보과학회지, 제23권 제12호, 2005. 12.제63면.

기술, 전환 프로세스를 설명한 전략적 정보자원의 기초가 된다. 기술참조모델은 업무 활동에 필요한 정보서비스를 식별하고 설명한 것으로 전사적 아키텍처의 모든 부문에서 고려된다. 참조 모델의 목적은 사용자 요구 사항을 만족시킬 수 있도록 시스템 규격에 대한 개념적인 모델을 추상화하는 것이다. 표준프로파일은 기술참조모델에 명시된 서비스를 지원하는 정보기술 표준들의 집합을 의미한다. 이러한 요소들에 디지털 포렌식의 속성과 목표를 반영할 때 새로운 디지털 포렌식 아키텍처가 구현되게 된다. 결국 앞서 종래의 디지털 포렌식 체계에서 설명이 곤란했던 사항들을 업무 프로세스의 모델의 범주의 상위의 계층의 차원에서 고려하고 이를 기술함으로써 문제해결을 시도하는 것이다. 상위계층에서의 변화는 하위계층에 매우 광범위하게 영향을 미치게 되므로 실질적으로는 전체적인 포렌식 체계에서 상당한 변화가 불가피하게 되는 것이다.

정보기술 아키텍처에서 정보시스템은 통합 및 표준화를 지향하게 된다. 정보시스템에는 최초 증거를 발견하고 수집하는 단계에서 최종적인 처리에 이르기까지 제공되는 각종의 서비스, 수집·생성되는 데이터, 이를 처리하는 업무 자체와 이에 사용되는 기술에 이르는 방대한 영역에 대한 정의와 검토를 필요로 한다. 이러한 시스템이 지향해야 할 바는 단순한 업무의 효율화로부터 법률이나 포렌식랩의 품질보증(Quality Assurance)을 위한 인증(Accreditation)제도에서의 요구들에 합치성을 포함하여야 할 것이다. 이것이 전통적인 단순 프로세스 기반의 디지털 포렌식에 대한 설명과의 차이이자 전통적 방식이 한계를 드러내는 이유이기도 하다.

아키텍처의 재사용가능한 구조를 가시화하기 위해서는 아키텍처 프레임워크(framework)를 구축하여야 하며 이에 대한 모델이 제시될 수 있는데, 조직적인 측면에서 보면 이러한 작업은 경찰청 차원에서 이루어져 지방에까지 적용되는 형태가 바람직할 것이다[112].

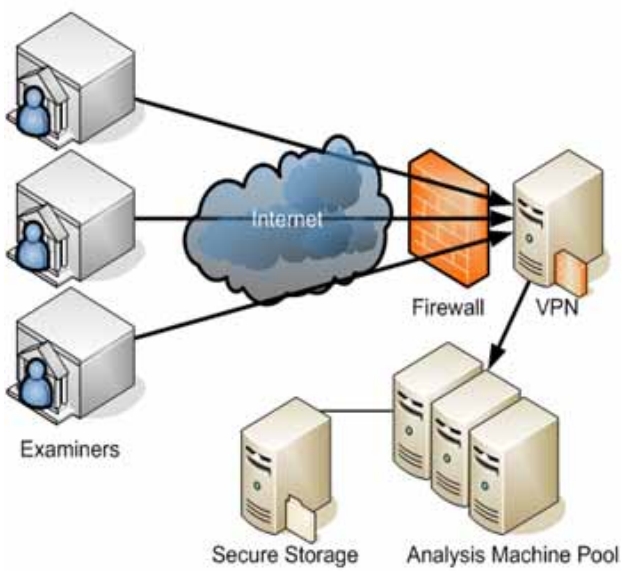
3. 미국 국립법과학연구소의 Virtual Digital Evidence Lab

미국 국립법과학연구소는 국립사법연구소의 지원을 받아 가상의 디지털 포렌식 랩을 설계하는 프로젝트를 진행하고 있다. 이 사업으로 인한 이점은 자원이나 작업의 불필요한

112) 장윤식, 전게 논문.

중복을 방지할 수 있으며, 자격있는 디지털 증거검사 전문가의 조력을 받을 수 있다는 것이다. 이 프로젝트를 진행함에 있어서 해결과제는 다음과 같은 것들이 제시되고 있다.

- 다수의 지리적 위치를 넘어서는 사용자 인증을 위한 최선의 방법을 찾는 것
- 공개적으로 접근 가능한 네트워크를 통해 원본 혹은 축소된 증거를 안전하게 전송하는 방법을 찾는 것
- 분산된 네트워크 환경에서 병목(bottleneck) 현상을 해소하는 것
- 디지털 포렌식 도구들에 대한 검증(validation)과 확인(verification)
- 검사관에 대한 원격지원의 방법
- 저장장치와 네트워트의 요구사항을 산출하고 시장성 문제를 해결하는 것



<그림 9> Virtual Digital Forensics Lab

(출처: http://www.ncfs.org/digital_evd.html#research)

제3절 Anti-Forensics 대응

포렌식 기술에 반하여 범죄자들은 자신의 증거들이 드러나지 않게 또한 많은 기술을 사

용한다. 가장 대표적인 것이 앞서 언급된 암호와 스테가노그라피와 같은 것들이며 최근에는 윈도우즈 기반의 데이터 완전삭제 프로그램이 일반인들에게까지 널리 사용되고 있다.

이러한 프로그램들은 인터넷 사용기록 등을 클릭 한번에 모두 삭제해 주거나 특정한 파일을 삭제하고 몇번이고 다른 데이터를 겹쳐 써 데이터 복구를 어렵게 하거나 혹은 삭제된 데이터를 암호화하여 현존하는 디지털 포렌식 기술을 무용한 것으로 만들기도 한다. 특별한 도구를 써서 완전하게 삭제된 파일을 되살리는 것은 매우 어려운 것으로 알려져 있어 그 대안으로 파일을 삭제하기 보다는 파일을 삭제한 흔적(trace)을 발견하는 기술 등이 연구되고 있다.[113]

제4절 유비쿼터스 컴퓨팅과 포렌식

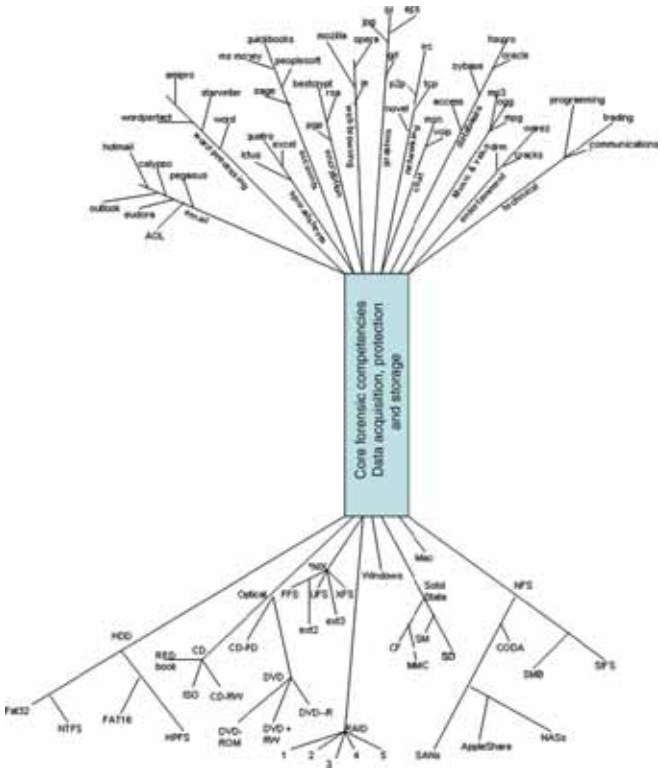
유비쿼터스 시대는 기존의 고정된 컴퓨터 네트워크를 넘어선 다양성, 융합성, 상시성, 이동성을 기반으로 한 네트워킹의 시대라고 할 수 있다. 다양한 매체에 들어 있는 IPv6는 종래의 IP 추적을 보다 어렵게 할 것이고 현재의 윈도우즈나 유닉스 계열 컴퓨터에 맞추어진 증거분석을 위한 파일시스템의 분석 필요성을 급증시킬 것이다.

<표 23> 유비쿼터스 신기술의 특징

끊김 없는 이동성 Seamless Mobility	어떤 기기를 사용하든 상관없이 언제 어디서나 필요한 정보를 얻을 수 있음
디지털 모바일화 Digital Mobilization	모든 물리적인 프로세스나 개인들의 접촉이 디지털 모바일화 됨
가상현실화 Virtual-Realization	가상으로 존재하는 데이터 또는 정보가 현실 공간으로 표현될 수 있는 가상현실화 됨
개인화된 단말장치 Personalized Device	개인을 중심으로 더 많은 서비스를 제공할 수 있도록, 디바이스가 개인화 됨
상황인지 Context Awareness	주변의 상황에서 일어나는 일에 대한 인지 능력이 있어야 함

113) http://www.ncfs.org/digital_evd.html#research 참조.

또한 더 이상 모든 매체에 대응할 수 있는 디지털 포렌식 전문가는 존재하기 어렵게 될 것이다. <그림 10>은 이러한 디지털 포렌식의 각 분야의 분화가 얼마나 심화될 것인가를 잘 나타내 준다. 지문 체계를 받아들인 것인지에 대한 논란은 있었지만 지문이 손가락에서 나온다는 사실이 변함없는 것에 반해 디지털 증거는 그 원천이 빠르게 변화한다는데 큰 문제가 있다.[114]



<그림 10> Tree analogy of technical complexity.

지금도 컴퓨터 뿐 아니라 PDA, 휴대전화, 손목시계 등 개인용 전자장치(personal electronic devices, PEDs)와 게임콘솔처럼 다양한 매체에 대한 포렌식 기술의 개발의 필요성이 있으나 그러한 기술의 개발이 진척되기도 이전에 더 빠른 속도로 새로운 형태의 디지털 장치들이 만들어지고 있다.

114) A. Sheldon, *"The future of forensic computing"*, Digital Investigation (2005), 2, 31-35.

제7장 차세대 디지털 포렌식 기반 구축을 위한 제언

제1절 미국 사례가 주는 교훈

디지털 포렌식과 관련된 랩의 설치나 전문인력의 양성, 관계되는 연구 등에는 막대한 자금이 소요된다. 미국은 우리나라보다 월등한 국가경제를 기반으로 많은 투자를 통해 디지털 포렌식을 발전시켜 나가고 있다. 하지만 모든 디지털 포렌식의 기반이 자금만으로 이루어진 것은 아니다. 미국에서 디지털 포렌식의 발달과정을 살펴보면 디지털 포렌식이 기존의 법과학의 토대 위에 자연스럽게 이식되고 있으며, 기존 법과학과의 차이점에 대해서는 법집행기관과 전문가들이 모여 기구를 형성하고 표준을 마련하는 등의 공감대를 빠르게 형성하며, 수요조사 등 기반연구를 선행하여 매우 체계적으로 그 기반을 하나하나 구축해 나가는 것을 볼 수 있다.

1. 국가적 과제로 인식

여러 사례에서 디지털 포렌식의 문제가 형사사법 서비스의 품질 및 정보기반시설의 보호 등 국가적 이해와 직결된 중요한 기능을 하여야 하며, 그러한 기능을 하기 위해 법과기술, 운영적인 각 측면에서 매우 어려운 과제들이 산적해 있음을 인식하고 디지털 증거의 특성을 고려하여 이에 대한 대책을 매우 광범위하게 수행하고 있음을 알 수 있다.

2. 기존 법과학계에의 참여

적용되는 세부적인 기술은 다르더라도 법과학에서 요구되는 품질보증을 위한 방법 등 많은 제도들은 디지털 포렌식에 그대로 적용될 수 있는 것이다. 기존의 틀 안에 디지털이라고 하는 특수한 분야를 추가하는 것은 모든 제도를 새로이 형성하는 것보다 훨씬 수월할 것이다. 많은 부분에서 표준화가 되지 않으면 공신력 있는 자격제도나 교육·훈련,

포렌식랩의 인증과 같은 핵심적인 기반들이 구축될 수 없음을 이미 기존의 법과학에서 경험한 많은 사람들이 알고 있었기에 최초의 관계기관간의 회의의 초점이 그것에 맞추어졌고 오래지 않아 그 성과를 이룰 수 있었던 것이다.

디지털포렌식 개념이 만들어진지 오래지 않아 디지털포렌식랩을 중심으로 실무조직이 재편되고 포렌식검사관에 대한 법과학 교육 등 제도가 마련되었으며, 인증제도에 디지털 포렌식을 포함시킨 후 곧 몇몇의 랩이 인증을 획득하는 등의 일련의 과정은 기존의 법과학계에서 만들어진 제도에 빠르게 적응하면서 법과학의 분야로서 디지털 포렌식 기반을 구축하는 모습을 잘 나타낸다.

아쉽게도 우리나라는 법과학이 국립과학수사연구소 등 몇몇의 특수한 기관에서 주로 다루어졌지 대학이나 일반화된 직업교육에서 그 흔적을 찾기가 매우 어려운 상황이다. 포렌식랩의 인증과 같은 제도들은 오랫동안 수사기관에 종사했던 사람들에게조차 매우 생소한 것들이다. 법과학을 발전시켜온 선진국에서 오랫동안 연구가 되어 왔던 법정에서의 증거능력 문제에 대처하기 위한 법과학계의 노력 또한 국내의 대부분의 사법기관 종사자나 관련 분야 전문가들에게 생소한 것들이다. 국내 형사증거법이 있음에도 미국의 법률과 판례를 보면서 증거의 채택가능성을 검토해야 하는 것들이 바로 그러한 문제에서 비롯된 것이라고 볼 수 있다.

3. 커뮤니티 중심의 협력체제 구축

SWGDE를 비롯한 단체들이 많은 다른 국가기관과 전문가들의 참여하에 만들어지고 이러한 단체들이 중심이 되어 여러가지 표준의 마련과 제도의 진화를 주도해 왔음에 주목할 필요가 있다. 이러한 모임들에 참여한 사람들은 자연스럽게 전문가 커뮤니티를 형성하고 그 분야에 대한 발전에서 중요한 역할을 한다. 예를 들어 위에서 언급한 TWGDE의 경우 40개 이상의 기관이 참여하고 있다. 참여기관에는 연방과 지방의 수사기관, 학계, 산업계, 비정부조직 등이 망라되어 있다.

이러한 조직들을 통한 공감대의 형성은 어떠한 결정을 하는데 있어서 합의의 도출에는 조금 더 시간이 걸릴 수 있지만 합의된 결과의 실천에서 그 비용을 충분히 보상받을 수 있을 것이다.

4. 활발한 기초연구

디지털 포렌식의 수요조사나 기술과 도구의 수요조사, 자격제도를 도입하는데 훈련 커리큘럼에 대한 조사 등은 많은 경우 국가의 재정지원을 받아 매우 체계적으로 이루어지고 있다. 이러한 기초조사는 실질적인 제도 정착의 기반이 되고 향후 연구의 중점방향을 선정하는 등 매우 다양한 형태로 활용될 수 있다.

제2절 국내 디지털 포렌식 기반에 대한 평가와 발전방향

미국을 중심으로 한 디지털 포렌식의 단계별 역사(태동기-확산기-정착기)에 비추어볼 때 현재 국내 디지털 포렌식 기반의 수준은 확산기에 막 진입한 수준에 머무르고 있는 것으로 판단된다. 디지털 포렌식랩이 만들어졌으나 아직 수사관과의 업무분담이 명확하게 이루어지지 않았으며, 전문가 커뮤니티가 막 형성되기 시작하였고, 표준에 대한 논의가 시작되고 법체계에 변화가 오기 시작한 것이 그렇다. 하지만 디지털 포렌식 검사관을 위한 체계적인 교육·훈련 및 자격제도, 포렌식랩의 품질관리 매뉴얼이나 인증제도의 부재 등 디지털 포렌식이 명실상부한 법과학의 한 분야로 인정받는 상태에 이르려면 아직 많은 난관이 있을 것으로 예상된다.

무엇보다 디지털 포렌식 서비스가 필요한 수요를 파악하고 이를 감당하고 있는가 하는 문제가 심각하게 고려되어야할 것으로 보인다. 앞에서 살펴본 바와 같이 미국의 경우와 비교해서 사이버범죄 등 디지털 포렌식 서비스 수요가 있을 것으로 예상되는 수치와 실제 제공되고 있는 서비스의 양은 매우 심한 격차를 보이고 있다. 이러한 격차는 경찰을 비롯한 디지털 포렌식의 소비자로부터 필요성에 대한 인식(awareness)이 필요함 또한 미국의 사례를 보아 확인된 바이나 설문조사에서 이러한 인식이 심각하게 부족한 상황임을 알 수 있었다. 이러한 문제점을 인식하고 변화를 이끌 수 있는 의사결정권자들은 이러한 문제에 심각한 주의를 기울여야 한다.

기존의 법과학과는 다른 새로운 개념의 법과학 기반이 필요함은 기존 포렌식랩 체제의 문제점이나 복합적이고 네트워크를 기반으로 하는 새로운 관점에서의 기술적 과제들이

산적해 있음도 확인할 수 있었다. 하지만 이러한 문제들에 대해 대비할 수 있는 연구자원과 지원은 찾아보기 어려운 상태이다. 지금의 발전속도와 인식의 수준으로는 향후 국민들이 기대하는 수준의 법과학 서비스를 제공하고 국제적인 경쟁력을 갖춘 디지털 포렌식 기반을 구축하는 것은 사실상 어려우며 따라서 지금까지의 사고의 틀을 바꾸어 차세대 디지털 포렌식 기반을 구축할 필요성이 절실하다.

세계 일류 수준의 IT기반과 우수한 인력을 보유하고 있는 우리에게 디지털포렌식은 다른 어떠한 법과학 분야보다도 빠른 시간 내에 선진국 수준에 도달할 수 있는 기회의 분야이기도 하다. 잠재적인 수요를 감당할 수 있는 충분한 서비스의 제공이라는 측면과 또한 법과 과학이 요구하고 있는 품질의 보증이라는 측면에서 향후 디지털 포렌식 기반의 구축방안이 설계되어야 할 것으로 보인다.

1. 디지털 포렌식 품질의 제고

미국의 경우 심지어 민간기업의 정보보안을 담당하는 부서에 속한 포렌식랩마저 랩인증을 추진하고 있다. 디지털증거를 분석한 결과는 범죄를 해결하는 등 서비스 수요자에 필요한 많은 정보를 제공한다. 하지만 그것이 법정에서 받아들여지지 않는다면 아무런 소용이 없다. 일반적으로 포렌식 검사결과가 법정에서 다투어진다면 확실히 그러한 정보가 나온 것인지 다투어질 것으로 생각되기 쉽상이다. 하지만 상대 변호사는 그런 질문을 하지 않고 예컨데 다음과 같은 질문을 한다고 한다.[115]

아무리 첨단의 기술을 사용하여 감추어진 증거를 찾아냈다고 하더라도 그 품질을 보증하기 위한 주변의 기반이 갖추어져 있는지가 그 결과에 대한 믿음을 바꾸어버릴 수 있다. 하지만 이러한 기반을 구축하는 것은 첨단의 기술을 배우고 익히는 것만큼 혹은 그 이상 노력이 필요한 것이다. 그것이 법과학이 추구해온 방향이며 우리가 추구해야할 방향이다.

115) J. Barbara, "*Digital evidence accreditation in the corporate and business environment*", Digital Investigation 2(2), June 2005, 137-146.에서 일부 발췌.

- 당신은 어떤 훈련을 받았나요
- Competency test(개인)와 Proficiency test(개인 및 조직)를 받았나요
- 분석과정에 관한 절차 매뉴얼이 있나요
- 그러한 절차는 검증된 것인가요
- 사용한 장비와 소프트웨어에 대한 표준과 통제절차를 준수하나요
- 사용한 소프트웨어에 결함이나 bug가 있는지 여부를 아는가요
- 소프트웨어 업데이트시 이에 대한 검증은 어떻게 하나요
- 증거분석을 한 장소에 어떤 사람들이 출입할 수 있나요
- 분석보고서에 대한 적절한 심사를 받았나요
- Computer Forensic 부서가 인증(accreditation)을 받았나요

2. 잠재적인 수요를 고려한 양적 기반의 확충

법률, 기술, 운영의 각 측면에서 많은 연구와 인력, 장비 및 도구가 필요하며 이를 위한 예산의 뒷받침 등 지원과 공동의 노력이 필요하다. 현재의 수요는 측정되지 않았고 앞으로의 수요는 예측하기 어렵다. 단순히 남이 만들어 놓은 기술과 장비를 들여와 사용하는 최종 소비자가 아니라 앞서나가고 수출하려는 노력이 필요하다.

제3절 차세대 디지털 포렌식 기반 구축을 위한 초기 실천 과제

많은 문제들은 문제에 대한 인식이 부족하기 보다는 그러한 문제들을 해결할 수 있는 구체적이고 체계적인 방법상의 문제일 수도 있다. 따라서 디지털 포렌식 기반의 발전을 이끌어내기 위해 구체적인 실천 방안을 모색해볼 필요가 있다. 특히 발전계획을 수립함에 있어 초기에 경찰청에서 참고할 수 있는 있다고 생각되는 사항들을 미국의 사례를 감안하여 간략히 정리해 보았다.

○ 선도연구 수행

- 우선적으로 전략적 마스터 플랜을 구축할 수 있는 조직을 편성할 것.
- 서비스, 장비나 도구, 연구, 인력, 예산 등의 실태와 수요분석(needs analysis)을 하고 그 격차를 비교(gap analysis)할 것. 미국에서 그와 같은 연구를 하는데만 부문별로 수년이 걸렸다는 것을 감안.
- 이러한 연구는 공신력 있는 연구기관에서 엄밀한 방법론을 적용하여 수행하도록 하고 그 결과를 공개하여 필요에 대한 인식을 확산시킬 것
- 관련되는 부서와 개인의 임무와 역할을 명확히 하여 부문별로 수요가 있는 부분이 명확하게 드러날 수 있게 할 것.
- 법과학의 기반을 형성하고 있는 제반 원리들을 파악하고 조화를 꾀할 것
- 향후 추세를 자체적으로 판단할 수 있도록 통계자료를 정기적으로 수집할 것.

○ 대내외 관심 및 지원 촉발

- 선도연구를 바탕으로 의사결정권자의 관심을 촉발하고 추가로 요구되는 예산을 신청하는 등 지원을 이끌어낼 것.
- 디지털 포렌식 발전이 형사사법 뿐 아니라 경제, 국가 및 기업보안 등 여러 영역에 관여되는 중요한 국가적 과제임을 인식하게 할 것
- 일반 경찰교육·훈련에서 디지털 포렌식 포함, 쉬운 교육자료 등을 통해 내부부터 존재를 각인시키고 수요를 드러나게 할 것

○ 전문가 커뮤니티 기반의 협력체제 구축

- 전문가 컴퓨니티의 중요성을 인식하고 이를 발전시키는데 지원할 것
- 결국 미국도 SWGDE 등 실무자, 전문가 커뮤니티가 제도 발전에 핵심적인 역할을 했음
- 경쟁관계보다 개방적 협력을 통해 상생관계를 형성할 것
- 조직으로 참여하기보다는 실무가나 전문가 등 개인으로 참여하여 장기적으로 논의의 흐름을 파악하고 주도적 역할을 수행하도록 할 것.

○ 조직의 정비

- 포렌식랩은 핵심시설 중의 하나로 지방청 이상에는 우선적으로 설치하되 제대로 된 하나가 급조된 여러 개보다 더 가치 있는 것임을 인식할 것. 법과학에서 포렌식랩은 단순히 증거분석이 이루어지는 곳 이상의 의미를 지님을 조직구성원 모두가 알게할 것.
- 준비없는 자격부여는 기득권층을 형성하여 향후 발전에 저해가 되며 이미 만들어진 포렌식랩에 형성되는 실무관행은 향후 변경하기 어렵게 됨
- 가능한 수준에서 디지털 포렌식 검사관(증거분석관)과 연구자, 수사관 등의 역할을 엄격하게 구분할 것
- 역할별로 임무를 명확하게 하고, 의사소통과 유기적 협력장치를 마련할 것
- 역할별로 전문성 개발 로드맵 및 장래 비전을 제시하여 동기를 부여할 것
- 계약직 연구원 시스템은 전문인력의 갑작스러운 누수 등으로 이어질 수 있으므로 장기적인 인력유치 계획을 수립할 것
- 포렌식 서비스의 영역을 명확하게 하고 인터넷 등을 통해 쉽게 파악할 수 있도록 공개할 것.

제8장 결 론

아직 신생분야이지만 국내외에서 관심이 증가하고 있는 디지털 포렌식 분야에 대한 전반적인 체계에 대해 선진국인 미국의 사례를 분석하여 그간 발전의 행적을 추적하고 이와 비교하여 국내의 실정과 문제점은 무엇인지 그리고 장기적인 관점에서 지향해야 할 방향과 실천적 추진방안을 모색해 보았다.

미국에서 디지털 포렌식은 수사관들의 필요에 의해 주도되다가 점차 법집행기관 출신자들이 주도적인 역할을 수행했던 전문가 집단을 필두로 포렌식랩을 중심으로 발전을 이루어왔다. 이 과정에서 수요분석 등 기반이 되는 국가주도의 핵심적 연구들이 존재하였으며 이를 토대로 법적·기술적·운영적 측면에서 요구사항 등을 조화시킬 수 있는 기반들이 차례로 형성되었음을 확인할 수 있었다. 이에 따라 그 기반요소를 수요, 법률, 조직운영, 포렌식랩 인증, 교육·훈련·자격제도, 적격성 및 숙련도 시험, 장비와 도구, 절차, 표준화, 연구 및 정보공유 등으로 구분하여 각각에 대해서 미국의 현재의 발전상태를 파악해 보았다. 이를 통해 각각의 요소들간의 조화를 이룰 수 있도록 하기 위한 조치들이 발전과정에서 꾸준히 논의되었으며, 지금은 ASCLD/LAB 인증(accreditation) 분야 지정, 국가적 자격 제도 시행시 지원자에게 필요한 지식·기술·능력에 대한 명세화, 숙련도 시험 기관 지정, 100개 이상의 대학의 교육 프로그램 제공 등을 통해 디지털 포렌식이 체계적인 법과학으로서 과학계와 교육계 모두의 인정을 획득하는 단계에 이르렀음을 확인할 수 있었다.

그와 같은 발전을 이루는데는 관련 전문가 커뮤니티의 매우 세부적이고 광범위한 사항에 대한 논의와 합의를 필요로 하는데 그나마 빠른 시간에 합의가 이루어진 것은 논의의 틀 자체가 기존의 발달된 법과학 제도에 의해서 제공되었기 때문으로 생각되었다. 반면 국내에서는 기존의 법과학 기반이 매우 허술하여 기술도입을 중심으로 필요에 의해 급격

하게 외국 특히 미국의 제도를 벤치마킹하고 있으나 제도의 밑바탕을 형성해야할 매우 기초적인 필요사항에 대한 체계적인 발전이 매우 더디게 진행되고 있는 상황이다. 종합적으로보아 아직 국내의 디지털 포렌식의 전반적인 발전상태는 미국의 디지털 포렌식의 발전기를 태동기-확산기-정착기로 구분했을 때 확산기의 초반부 정도에 그치고 있는 것으로 판단되었다.

게다가 미국과 비교했을 때 이러한 발전 속도는 글로벌한 경쟁에 나서기에는 법과학 서비스의 품질보증이나 수요를 충족하는 질과 양적 측면 모두에서 부족하여 혁신적인 변화를 필요로 하며 이를 위해 무엇보다 국가적인 인식의 제고가 필요하다는 결론에 이를 수 있었다. 덧붙여 기존의 것들과 큰 틀에서의 변화의 필요성을 발견하고 국가적 규모의 투자를 필요로 하는 정보시스템 기반의 디지털 포렌식 아키텍쳐 개발 등 새로운 기술적 연구・개발 분야를 파악하였다. 마지막으로 이른바 차세대 디지털 포렌식 기반 구축이라는 주제를 실현할 수 있는 실천방안을 나름대로 제시해 보았다.

디지털 포렌식은 형사소송법의 개정이나 자유무역협정 체결, 새로운 IT환경, 범죄양상의 변화 및 과학적 수사방법에 대한 국민의 요구 증가와 같은 매우 큰 변화들의 한 가운데에 있는 분야로 이를 어떻게 적절하게 발전시키느냐가 형사사법 서비스의 질을 결정짓는 매우 중요한 요소가 될 전망이며 우리나라는 법과학의 기반이 부족한 반면 IT기반은 어느 선진국에 뒤떨어지지 않는 수준에 이르고 있으므로 노력여하에 따라 얼마든지 이 분야에 대한 발전을 선도할 수 있는 국제적 경쟁력을 갖출 수 있을 것으로 보인다. 아무쪼록 이 연구가 이러한 발전에 조금이나마 보탬이 되기를 기대한다.

참 고 문 헌

1. 국내 문헌

신신애, “EA(Enterprise Architecture)기반 표준화 추진 방안”, 정보과학회지, 제23권 제12호, 2005. 12.

심희기, “과학적 증거의 허용성과 신빙성”, 고시계 제514호:5-15, 1999. 11.

양근원, 형사절차상 디지털 증거의 수집과 증거능력에 관한 연구, 경희대학교 박사학위 논문, 2006.

이상수 등, “대용량 저장 매체를 고려한 디스크 이미지 포맷”, 제1회 안티포렌식 대응기술 워크샵, 한국정보보호학회/한국디지털포렌식학회, 67-76, 2007. 8.

이성진, “디지털 포렌식스 기술 발전 방안”, 디지털포렌식연구 창간호:1-22, 2007. 11.

임종인, “유비쿼터스 시대의 컴퓨터 포렌식의 중요성과 향후 전망”, 수사연구 2005년 3월호:12-16.

임종인・박종환, “사이버범죄방지조약의 절차규정에 관한 연구”, Information Security Review, 창간호, 2004.

임준태, 과학수사기반 구축을 위한 법과학교육 활성화, 한국경찰학회보, Vol 14, 3-42, 2007.

장윤식, “정보기술 아키텍처 기반의 디지털 포렌식 체계 도입에 대한 연구”, 경찰학연구, 7(2):65-84, 2007.

_____, “범죄연구실 중심의 미국 과학수사 현황”, 경찰학연구, 7(2):271-280, 2007.

탁희성, “법정에서 디지털 증거의 허용가능성”, 디지털포렌식연구 창간호:23-41, 2007. 11.

한면수 외, 과학수사론, 경찰대학, 2007.

2. 외국 문헌

A. Sheldon, “The future of forensic computing”, Digital Investigation (2005), 2, 31-35.

AAFS Forensic Science Education Programs Accredatation Commission, “Accreditation Standards” (http://www.aafs.org/pdf/FEPAC%20 Accreditation%20 Standards%20_082307_.pdf), August 23, 2007.

B. Carrier and E. Spafford, “Getting Physical with the Digital Investigation Process”, International Journal of Digital Evidence, Fall 2003 2(2):7-10.

B. Carrier and E. Spafford. “Getting physical with the digital forensics investigation”, International Journal of Digital Evidence 2003:2(2).

B. Reaves and M. Hickman, Census of state and local law enforcement agencies, 2000, Bureau of Justice Statistics Bulletin, NCJ 194066, U.S. Department of Justice, Washington, DC (www.ojp.usdoj.gov/bjs/ pub/pdf/cslleaOO.pdf), 2002.

B. Schneier, Secrets & Lies: Digital Security in a Networked World, John Wiley & Sons, 2000.

Bill Nelson, et.al., “Computer Forensics and Investigations”, Tompson, 2004.

Bureau of Justice Statistics(BJS), 50 Largest Crime Labs 2002, 2002

Bureau of Justice Statistics, Census of Publicly Funded Forensic Crime Laboratories, 2002, (http://www.ojp.usdoj.gov/bjs/pub/pdf/cpffcl02.pdf), 2005.

C. Taylor, B. Endicott-Popovsky, A. Phillips, “Forensics Education: Assessment and Measures of Excellence”, proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2007), 155-165, 2007.

C. Taylor, B. Endicott-Popovsky, A. Phillips, Ibid. ???

C. Whitcomb, “An Historical Perspective of Digital Evidence: A Forensic Scientist's View”, International Journal of Digital Evidence, Spring 2002 1(1).

CCIPS, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, (http://www.cybercrime.gov/s&smanual2002.htm), July 2002.

D. Shinder, Scene of The Cybercrime: Computer Forensic Handbook, Syngress, 2002.

E. Appel and M. Pollitt, Report on the Digital Evidence Needs Survery of State, Local, and Tribal Law Enforcement, (http://www.jciac.org/docs/Digital%20Evidence%20Survey%20Report.pdf), 2005.

G. Palmer, “A Road Map for Digital Forensic Research. Technical Report DTR-T0010-01”, DFRWS, November 2001. Report from the First Digital Forensic Research Workshop (DFRWS).

H. Stambaugh, et. al., “State and local law enforcement needs to combat electronic crime”, National Institute of Justice Research in Brief, 2001.

H. Wolfe, “Setting up and electronic evidence forensics laboratory”, Computer & Security vol22, No8, Elsevier, (http://www.compseconline.com/hottopics/hottopic_Feb04/settingupaforensicsunit.pdf), 2003.

Institute for Security Technology Studies, “Law Enforcement Tools and Technologies for Investigating Cyber Attacks”, (http://www.ists.dartmouth.edu/TAG/needs/ISTS_NA.pdf), 2002.

Institute for Security Technology Studies, “Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report”

Institute for Security Technology Studies, “Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis

Report", (http://www.ists.dartmouth.edu/TAG/gar/ISTSGapAnalysis 2004.pdf), 2004.

Institute for Security Technology Studies, "Law Enforcement Tools and Technologies for Investigating Cyber Attacks: National Research and Development Agenda" http://www.ists.dartmouth.edu/TAG/agenda/ ISTS_NRDA0604.pdf, 2004.

Internet Crime Complaint Center, 2006 Internet Crime Report, (http:// www.ic3.gov/media/annualreport/2006_IC3Report.pdf), 2007.

J. Barbara, "Digital Evidence Accreditation", Forensic Magazine,, (http:// www.forensicmag.com/articles.asp?pid=21), Winter 2004.

J. Barbara, "Digital evidence accreditation in the corporate and business environment", Digital Investigation 2(2), June 2005, 137-146.

J. Ladyman(박영태 옮김), 과학철학의 이해, 이학사, 2003.

J. Stuart and J. Nordby, Forensic Science: An Introduction to Scientific and Investigative Techniques, CRC, 2002.

K. Meadaris, "Grants to help develop ways to improve digital evidence collection", Purdue University, (http://www.purdue.edu/UNS/html4ever/ 2006/061012RogersGrant.html), Oct. 2006.

M. Meyers, M. Rogers, "Computer Forensics: The Need for Standardization and Certification", International Journal of Digital Evidence, 3(2), 2004.

M. Pollitt, "Who is SWGDE and what is the history?", (http:// 68.156.151.124 /SWGDE_History.pdf), 2003.

M. Rogers, et al., "Survey of Law Enforcement Perceprtion Regarding Digital Evidence", 2007, in IFIP International Federation for Information Processing, Volume 242, Advances in Digital Forensics Ⅲ; eds. P.Craiger and S Shenoi;(Boston: Springer).

M. Rogers, K. Seigfried, The future of computer forensics: a needs

analysis survey, Computer & Security(2004), 23, Elsevier, 12-16.

M. Rogers, K. Seigfried, The future of computer forensics: a needs analysis survey, Computer & Security(2004), 23, Elsevier, 12-16.

M. Rogerts and K. Seigfried, “The Future of Computer Forensics: a needs analysis survey”, Computers & Security 23:12-16, 2004.

M. Simon and J. Slay, “Forensic Computing Training, Certification and Accreditation:An Australian Overview”, in IFIP International Federation for Information Processing, 237, Fifth World Conference on Information Security Education, eds. Futcher, L., Dodge, R., (Boston: Springer).

M. Simon, J. Slay, “Forensic Computing Training, Certification and Accreditation: An Australian Overview”, in IFIP International Federation for Information Processing, Volume 237, Fifth World Conference on Information Security Education, eds. Futcher, L., Dodge, R., (Boston: Springer), 2007.

NIJ, “Education and Training in Forensic Science: A Guide for Forensic Science Laboratories, Educational Institutions, and Students” (http://www.aafs.org/pdf/NIJReport.pdf), June 2004.

NIJ, Status and Needs of Forensic Science Service Providers: A Report to Congress, (http://www.ncjrs.gov/pdffiles1/nij/213420.pdf), March 2006.

NIJ, Status and Needs of Forensic Science Service Providers: A Report to Congress, March 2006, NCJ 213420, (http://www.ncjrs.gov/pdffiles1/nij/213420.pdf).

P. De Forest, R. Gaensslen, and H. Lee, Forensic Science: An Introduction to Criminalistics, McGrow-Hill, 1983.

P. Rice, Electronic Evidence: Law and Practice, American Bar Association, 2005.

R. McKemmish, What is Forensic Computing? Australian Institute of

Criminology Trends and Issues 118, (http://www.aic.gov.au/publications/tandi/ti118.pdf), 1999.

R. Saferstein, Criminalistics: An instruction to forensic science 9th Edition, Pearson Prentice Hall, 2007.

Regional Computer Forensic Laboratory, RCFL Program Annual Report for Fiscal Year 2006, (http://www.rcfl.gov/downloads/documents/RCFL_Nat_Annual06.pdf), 2007.

S. Hilley, US cybercrime statistics: FBI hotline gets more than 200,000 complaints, Digital Investigation, 4(2007) 54-55.

T. Owen, et. al., "Law and The Expert Witness-The Admissibility of Recorded Evidence", AES 26th International Confernece, (http://www.owlinvestigations.com/LawandtheExpert WitnessDenver05paper.pdf), July 2005

T. Wilsdon, J. Slay, "Digital forensics: exploring validation, verification & certification" Systematic Approaches to Digital Forensic Engineering, 2005. First International Workshop on , vol., no., pp. 48-55, 7-9 Nov. 2005

The National Center for Forensic Science The Certification Roundtable Meeting, Draft Final Report, (http://www.ncfs.org/dfcb/CERT%20ROUNDTABLE%20REPORT%20(DRAFT%20V% 206-07-04).pdf.), 2006.

U.S. Department of Justice, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement", 2004.

US Department of Justice, 2008 Budget and Performance Summary, (http://www.usdoj.gov/jmd/2008summary/html/107_fbi.htm), 2007.

US Department of Justice, Audit of the Department Justice Information Technology Studies, Plans, and Evaluations, (http://www.usdoj.gov/oig/reports/plus/a0739/final.pdf), August 2007.

W. Ren, "Modeling Network Forensics Behavior", Journal of Digital Forensic Practice 1:57-65.

부 록

<부록 1>

◎ 디지털 포렌식 관련 주요 단체

○ American Academy of Forensic Sciences (AAFS)
○ American Society of Crime Laboratory Directors (ASCLD)
○ Digital Detective Forum (DDF)
○ Electronic Crime Partnership Initiative (ECPI)
○ Forensic Association of Computer Technologists (FACT)
○ High Technology Crime Consortium (HTCC)
○ High Technology Crime Investigation Association (HTCIA)
○ International Association of Computer Investigative Specialists (IACIS)
○ International Organization on Computer Evidence (IOCE)
○ International Police Organization (Interpol)

◎ 디지털 포렌식 관련 기술·과학 워킹그룹

○ Digital Forensics Research Workshop (DFRWS)
○ Digital Forensics Working Group (DFWG)
○ International Federation of Information Processing Working Group 11.9 on Digital Forensics (IFIP WG 11.9)
○ Scientific Working Group on Digital Evidence (SWGDE)
○ Scientific Working Group on Imaging Technologies (SWGIT)
○ Electronic Crime Partnership Initiative (ECPI) - National Institute of Justice
  - Tools and Technology Working Group
  - Awareness and Outreach Working Group
  - Policy and Legal Working Group
  - Standards and Certification Working Group
  - Technical Assistance Working Group Education and Training Working Group

<부록 2>

전미 법과학시험기관장 협회 랩 인증 위원회 매뉴얼

(발췌 번역)
American Society of Crime Laboratory Directors
Laboratory Accreditation Board
Manual

표준과 평가기준
(각 항목 앞에 영어 대문자로 표기된 것)
essential(E) - 100% 충족하여야 함
important(I) - 75% 이상 충족하여야 함
desirable(D) - 50% 이상 충족하여야 함

1. 랩 경영과 운영

1.1. 기획(Planning)

1.1.1 목 적

○ 원칙

경영은 어떠한 다른 활동의 이전에 목표가 명확하게 결정되고, 구분되고 이해될 때 보다 효과적이다.

○ 표준과 평가기준

랩은 구성원 모두에게 구두와 문서로 설명된 목표를 설정하여야 한다.

(I) 랩은 문서화된 목표를 가지고 있는가

(I) 목표는 랩이 서비스를 제공하고자 하는 지역사회의 필요와 관련된 것인가

(D) 랩의 운영진은 이 목표를 이해하고 지원하는가

1.1.2. 행정적 책략

○ 원 칙

구성원의 관리적 기능의 효율성은 행정적 책략(administrative practices)이 논리적으로 개발되고, 명확하게 기술되며, 전달될 때 향상된다

○ 표준과 평가기준

랩 혹은 상위기관은 포렌식 서비스에 상응하는 공식적으로 작성된 예산을 지니고 있어야 한다

(I) 랩 혹은 상위기관은 공식적으로 기록된 예산을 지니고 있는가

(I) 그 예산은 작성되어 있는 목표를 달성하기에 충분한가

다음 사항에 대해 명확하게 기술되고 구성원들에게 잘 이해가 되어 있는 문서 혹은 절차가 존재하는가

(E) 증거의 무결성 처리와 보존?

(E) 랩 보안?

(E) 사건기록 및 보고서의 준비, 저장, 보안과 반출?

(E) 물질과 공급품의 통제?

(E) 장비와 도구의 유지, 교정

(E) 개별 특성 DB의 운영?

(D) Job 요건과 이에 대한 기술

(D) 개인 평가와 목표?

(D) 품질시스템과 관련된 구성원 불만(complaint)?

랩은 목표를 수행하는 것을 도와줄 관리정보시스템을 보유하여야 한다
(I) 랩은 경영정보시스템(MIS)를 보유하고 활용하는가?

1.2. 조직구성

업무를 특정하고 업무와 자원을 구조내에 그룹화하고, 업무를 할당하고, 개인과 그룹간의 명령의 연계성을 확보하는 절차

1.2.1. 조직 구조

○ 원 칙

조직은 업무와 자원을 그룹화할 때 구성원의 수, 구성원간의 상호작용, 의사결정의 수준, 개인과 조직 목표의 합치 등과 같은 상호적 변수가 완전하게 고려될 때 효과적, 효율적이다.

○ 표준과 평가기준

랩관리자는 원칙에 언급된 것과 같은 상호관련된 변수들 속에 조직구조를 연결할 수 있어야 한다

(D) 조직구조가 다양한 포렌식의 원칙들간의 관련을 고려하여 작업의 효율성을 확보할 수 있도록 업무와 구성원들을 그룹짓는가.

(D) 랩 책임자는 업무와 자원을 그룹핑할 때 구성원의 숫자간의 불균형을 수정할 수 있도록 고려하여 적절한 조치를 취하였나

・논 의 : 포렌식랩을 위한 단일한 완벽한 조직은 존재하지 않는다. 열거된 변수들을

고려하면 조직은 효과적으로 구성될 것이다.

1.2.2. 권한 부여

○ 원 칙

랩이 목표를 달성하려면 책임자는 결정을 하고 이를 실행할 수 있는 충분한 권한을 지니고 있어야 한다. 효과적인 조직은 부여된 책임, 책임추적성의 보증, 지시의 일치성, 확고한 수행 평가기준과 상응하는 권한의 위임을 필요로 한다.

○ 표준과 평가기준

랩 책임자는 부여된 책임에 상응하는 권한을 지니고 있어야 한다.
(I) 랩 책임자의 권한은 잘 규정되어 있는가?
(I) 랩 책임자는 책임에 상응하는 권한을 지니고 있는가?

・논 의 : 모든 조직에서 특정한 기능의 효율적이고 효과적인 수행을 위한 책임이 부여되어야 한다. 이러한 책임이 부여될 때는 이에 상용하는 실행 혹은 타인의 실행을 지시할 수 있는 적절하고, 잘 규정된 권한이 부여되어야 한다. 책임자가 랩의 임무를 달성할 수 있는 권한을 지니고 있지 않다면 효과적인 조직이 구성될 수 없다.

랩 내에서 권한의 위임은 원칙에서 제시된 조직적 프로세스를 따라야 한다.
(I) 충분한 권한 위임이 이루어져 있는가?
(I) 감독자들의 권한은 책임에 상응한가?
(I) 각각의 부하직원들은 기능별로 단일한 감독자에 대해 책임지는가?
(I) 작업수행 기대치가 수립되어 있으며 그것이 랩 구성원들에게 이해되어 있는가?

・논의 : 관리적인 책임이 범위와 복잡성이 증가함에 따라 조직을 통한 권한의 위임 하향화는 필수적인 것이 되었다. 랩은 직원들의 지식과 능력의 최대치를 보장할 수

있는 조직구조를 지녀야 한다. 가능한 최저 수준으로의 권한위임이 이러한 목표를 달성하게 한다. 하지만 모든 직원들이 어떤 것을 할 것을 기대받고 있는 지를 명확하게 이해하는 것이 중요하다.

1.3. 관리감독(directing)

동기부여를 부여하고 지휘(lead)와 지도(guide)를 하는 과정

1.3.1. 감 독

○ 원 칙

좋은 감독은 창조적인 발상과 객관성의 유지, 비평적으로 프로그램을 평가하는 것을 촉진한다.

○ 표준과 평가기준

건설적인 토론이 감독자와 부하직원간에 있어야 한다
(D) 감독자와 부하직원간의 건설적인 토론이 있는가

감독자는 주의 깊고 객관적으로 랩의 활동과 인원들을 검토하여야 한다.
(I) 감독자들은 주의 깊고 객관적으로 랩의 활동과 인원들에 대해 검토하는가

감독 기술은 창조적인 사고와 객관성을 북돋고 부하직원들의 공적에 대해 인식할 수 있어야 한다
감독 기술은 창조적 사고와 객관성을 북돋고 부하직원들의 공적에 대한 인식하고 있는가

・논의 : 조직의 업무수행의 기본은 능력과 그것을 실행하려고 하는 직원들의 열망에 있다. 아이디어가 억제된다면 조직은 정체될 것이다. 객관성이 충분하지 않다면 시

스템은 균형을 잃고 개인들은 불만족하게 된다. 직원과 활동에 대한 주의 깊은 검토가 없다면 랩서비스의 품질은 훼손될 수 있다. 특출한 업무수행은 이행을 촉발할 수 있도록 인식되어야 한다. 좋지 못한 업무 수행 또한 인식되어야 하며 문제를 해결하기 위한 개인들의 협동을 이끌어낼 수 있는 긍정적 접근이 사용되어야 한다. 이러한 협조는 앞으로 기대되는 것이 아니라 감독자가 실행에 옮길 책임이 있다.

1.3.2. 커뮤니케이션

○ 원 칙

모든 커뮤니케이션은 효과적이기 위해 명확하고 간결하며 아이디어의 교환을 활성화하여야 한다.

○ 표준과 평가기준

사건처리 조정과 기술 및 작업정보의 광범위한 배포를 보증할 수 있도록 랩 내에서의 커뮤니케이션이 존재하여야 한다.

(D) 랩 내에 효과적인 커뮤니케이션 수단이 존재하는가?

・논의 : 효과적인 업무수행에 있어 좋은 커뮤니케이션은 필수적이다. 모든 수준에서의 정보의 교환은 조직의 목표 달성에 도움이 된다. 정보는 제 때에 제공되어야 하며 토론할 수 있도록 개방되어야 한다. 랩 구성원에 있어 정보의 커뮤니케이션은 많은 매커니즘에 의해 달성될 수 있다. 서면화된 커뮤니케이션이 검토를 위해 알기 쉽게 유지되어야 한다. 랩 구성원의 개방형 커뮤니케이션을 위한 정기적인 직원 회의는 좋은 수단이 된다.

1.3.3. 훈련과 개발

○ 원 칙

직원의 훈련과 개발은 정확성을 향상시키고, 생산성을 높이며 책임감을 높일 수 있도

록 강조되어야 한다.

○ 표준과 평가기준

모든 응용분야와 그 하위분야에 있어 훈련 프로그램은 구성원의 기술을 개발하는데 있어 필수적이다.

(E) 랩은 각 분야에 하위분야별로 신규와 훈련받지 않았거나 교정적 훈련을 받아야 할 필요성이 있는 구성원에 대해 문서화된 훈련 프로그램을 지니고 활용하고 있는가?

공식화된 개인 능력개발 프로그램은 구성원이 좀 더 책임 있는 일을 감당할 수 있도록 하는데 중요하다.

(I) 랩은 직원들의 능력개발 프로그램을 가지고 있는가?

랩은 응용가능한 기능 분야에 있어 출간물을 보유할 수 있는 충분한 법과학 도서관을 유지하여야 한다.

(I) 법과학 도서관은 서적과 저널 및 각각의 기능분야를 취급하는 출간물을 보유하고 있는가?

구성원들이 적절하게 새로운 출간물들을 검토해볼 수 있는 시스템과 절차를 지니고 있는가?

(I) 각각의 검사관들이 적절한 새 출간물들을 검토해볼 수 있는 시스템이 존재하는가?

1.4. 통 제

업무수행 표준을 수행하고 현재의 수행력을 측정하며 필요한만큼 지속적인 향상을 보증

1.4.1. 증거와 개별특성 DB 표본통제

○ 원 칙

통제시스템은 증거의 무결성을 개별적인 특성 DB 표준을 보증하고 문서화될 때 효과적으로 설계된다.

○ 표준과 평가기준

종합적이고 문서화된 랩이 처리하는 개별 증거이송 역사를 제공하는 증거확보연계(a chain of custody) 기록이 유지되어야 한다.

(E) 랩은 모든 증거의 완전한 추적을 제공하는데 필요한 모든 필요한 데이터를 포함하는 문서화된 혹은 안전한 전자적 증거확보연계 기록을 가지고 있는가?

- 논의 : 각각의 개별 증거품들은 실무적으로 가능할 때 식별할 수 있도록 표시가 되어야 한다. 증거품 자체에 표시를 하는 것이 적절하지 않을 경우 증거물에 가장 가까운 용기나 식별태그에 표기되어야 한다.

(E) 모든 증거는 식별을 위한 표시가 되어 있는가?

- 논의 : 증거에 대한 봉인이 디자인되고 증거의 무결성을 보호하기 위해 활용되어야 한다.

(E) 증거는 적절한 봉인 하에 보관되고 있는가?

- 논의 : 증거에 대한 망실과 교차 이송, 오염 등 잘못된 변화의 위험을 줄일 수 있도록 절차적 예방수단이 존재하여야 한다.

(E) 증거는 망실이나 교차 이송, 오염 등 잘못된 변화로부터 보호되고 있는가

- 논의 : 디지털, 멀티미디어 증거를 검사하기 위해 사용되는 컴퓨터시스템은 네트워크에 연결되어 있다면 부정접속에 취약할 수 있으며 시스템을 보호하기 위해 적절한

수단이 활용되어야 한다. 덧붙여, 미디어나 이메일의 도중에 바이러스가 유포될 수도 있다. 디지털과 멀티미디어 증거의 검사에 사용되는 컴퓨터시스템의 검증되지 않은 미디어와 이메일은 최신의 안티바이러스 프로그램으로 검사하여야 한다.

증거물의 야간, 장기 보관을 안전한 공간이 활용 가능하여야 한다.
(E) 증거물의 야간, 장기보관을 위한 안전한 장소가 확보되어 있는가?

랩은 개별 특성 DB 표본이 증거, 참조 자료 혹은 검사 문서로 다루어질 수 있도록 하여야 한다.
(E) 랩은 개별적인 특성화 DB 표본이 증거, 참조 자료, 혹은 검사문사로 다루어질 수 있도록 하고 있는가?

랩의 통제 하에 있는 개별 특성 DB 표본 은 유일하게 식별되어야 한다.
(E) 랩의 통제 하에 있는 개별적인 특성DB 표본는 유일하게 식별되고 있는가?

개별 특성 DB 표본이 망실, 교차 이송, 오염 등 잘못된 변화의 위험을 줄이기 위한 절차적인 예방조치가 존재하여야 한다.
(E) 개별 특성 DB 표본이 망실, 교차 이송, 오염 등 잘못된 변화로부터 보호되고 있는가?

랩의 통제하에 있는 개별 특성 DB 표본에 대한 접근은 랩 책임자로부터 승인받은 사람들에게만 제한적으로 허용되어야 한다.
(E) 랩의 통제하에 있는 개별 특성 DB 표본에 대한 접근은 랩 책임자로부터 승인받은 사람들에게만 제한적으로 허용되고 있는가?

1.4.2. 품질 시스템

○ 원 칙

보고된 결과와 결론의 유효성을 강화하기 위해 랩은 해당 법과학 분야의 범위 뿐 아니라 수행되는 검사의 유형과 수에 적합한 품질 시스템을 갖추어야 한다.

○ 표준과 평가기준

랩의 모든 품질시스템의 요소들은 품질관리관(quality manager)의 책임 하에 최신의 품질매뉴얼에 명확하게 문서화되어 있어야 한다.

(E) 랩은 종합적인 품질 매뉴얼을 보유하고 있는가?

・논의 : 종합적인 품질 매뉴얼은 다음과 같은 내용을 포함하는 문서나 정책/절차를 포함하거나 참조토록 하여야 한다.

경영차원에서 목표와 수행을 포함하는 품질 정책에 대한 기술

랩의 조직 및 경영구조, 상위조직에서의 위치와 관련된 조직 차트

품질 시스템을 적용하는데 있어서 경영, 기술적 운영과 지원서비스간의 관계와 책임

작업에 대한 기술, 교육, 그리고 랩 운영진에 대한 최신의 훈련 기록

사건 기록과 절차 매뉴얼의 문서 통제와 유지

가능한 경우 측정을 통해 표준에 적합한 지를 보증할 수 있는 랩의 절차

랩에 의해 수행되는 검사의 유형과 정도

검사절차의 검증

증거의 취급

랩 절차에 있어 표준과 통제의 활용

장비의 교정과 유지

랩간의 비교, 숙련도 검사 프로그램, 기술적인 검토 등 내부의 품질 통제 절차를 통한 검사관들의 능력의 지속을 보증할 수 있는 실천적 수단

분석적 편차(analytical discrepancies)가 발견되었을 때마다 교정 조치

과학적 발견의 보고가 편견 없고 효과적인 방법으로 되었는지를 보증하기 위한 법정 증언의 모니터링

문서화된 정책과 절차를 벗어나는 것을 허가할 때의 랩 프로토콜

정보의 공개
감사와 품질시스템 검토

랩은 지정된 품질관리관이 있어야 한다.
(E) 품질관리관으로 지정된 자가 있는가?

・논의 : 품질관리관의 임무
품질 매뉴얼의 유지와 업데이트
랩의 실무처리가 정책과 절차에 부합하는지 모니터
도구의 교정과 유지기록에 대한 평가
보고서 검토 활동의 적합성에 대한 정기적 평가
새로운 기술적 절차에 대한 유효성 검증을 보장
기술적 문제에 대한 조사, 교정적 조치를 제안하고 그것을 적용한 것에 대한 검증
숙련도 검사의 운영과 결과의 평가
내부 감사의 선정, 훈련과 평가
품질시스템 감사의 스케줄링과 조정
랩 구성원의 훈련 기록의 유지
랩 인력의 자질을 향상시키기 위한 훈련의 추천
품질 시스템의 교정과 향상의 제안

인증된 랩에서는 그 업무수행이 품질시스템의 요구 및 ASCLD/LAB 인증의 표준에 지속적으로 부합하는지를 검증하기 위해서 연례 감사를 실시하고 그 결과를 소정의 양식에 의해 ASCLD/LAB에 제출하여야 한다.

(E) 인증된 랩은 연례 감사를 시행, 기록하고 ASCLD/LAB에 정해진 기간까지 감사 보고서를 제출하였는가?

・논의
(세부 내용 생략)
감사 체크리스트

직원의 품질 매뉴얼에 대한 인식
분석적 절차 선택, 통제와 검증(validation)
시약과 표준의 통제
장비의 교정 및 관리 기록
사건 보고서, 노트 및 정리의 충분함
증거취급 절차
숙련도 테스트와 랩간 비교 검토
개인 훈련 기록
흠결의 처리와 개선책
랩의 질서와 건강 및 안전 측정

품질 시스템은 최소 일년에 한번 지속적인 품질시스템에의 적합성과 효과성을 보증하기 위해 랩 경영 검토를 요한다.
(E) 랩은 연례 품질시스템 검토를 시행하고 문서화하는가?

절차는 그 분야에서 일반적으로 받아들여지는 방법을 사용하거나 과학적인 방법으로 수집되고 기록된 데이터에 의해 지지되어야 한다.
(E) 절차는 그 분야에서 일반적으로 받아들여지거나 과학적인 방법으로 수집, 기록된 데이터에 의해 지지되는가?
새로운 기술적 절차는 실제 사건에 적용되기 이전에 증거검사에의 유효성을 증명하기 위해 검증되어야 한다.
(E) 새로운 기술적 절차는 실제 사건에서 사용되기 이전에 과학적으로 검증되고 그 검증 문서가 검토 가능한가?
랩은 적절한 기술적 절차에 대한 기록된 사본을 보유하여야 한다.
(E) 랩에서 사용되는 기술적 절차는 문서화되었으며 그 문서는 랩의 구성원이 검토할 수 있는가?
검사 요인과 결과에 대한 유효성을 보증하기 위해 사건기록에는 통제와 표준 표준이 사용, 기록되어야 한다.

(E) 절차에는 적절한 통제와 표준이 특정화되어 있는가, 또한 검사결과의 유효성을 보증하기 위해 사건기록에 활용되고 기록되는가?

표준 표본과 시약의 품질은 사용된 절차에 적합한 것이어야 한다.

(E) 표준 표본과 시약의 품질은 사용된 절차에 적합한 가?

모든 시약은 신뢰성에 대한 정규적인 검사가 이루어져야 한다.

(E) 랩은 정규적으로 시약에 대한 신뢰성을 검사하는가?

도구/장비는 사용된 절차에 적합하여야 한다.

(E) 도구/장비는 사용된 절차에 적합하여야 한가?

도구/장비는 적절한 작업명령에 의해 유지되어야 한다.

(I) 도구/장비는 적절한 작업명령 내에 있는가?

도구/장비는 적절하게 교정되고 교정 기록이 유지되어야 한다.

(E) 도구/장비는 적절하게 교정되고 있는가?

랩은 증거에 대한 분석을 포함한 모든 사건에 대해서 생산하거나 수령한 모든 행정과 검사 문서를 위해 유일하게 식별된 사건기록을 작성, 유지하여야 한다.

(E) 랩은 증거에 대한 분석을 포함한 모든 사건에 대해서 생산하거나 수령한 모든 행정과 검사 문서를 위해 유일하게 식별된 사건기록을 작성, 유지하는가?

랩의 독자적인 사건 식별기호가 매 검사 문서의 면마다 표시되어 있어야 하며, 그 문서를 작성한 사람이 자신이 작성한 면에 수기 이니셜 혹은 이에 상응하는 안전한 전자적인 표시를 나타내야 한다

(E) 각각의 검사 문서 페이지에는 랩의 유일한 사건 식별기호가 나타나는가 또한 검사문서를 생산하는 자의 수기 서명(initial)이나 안전한 전자서명이 각각의 페이지에 나타나는가?

(E) 보고서의 결론과 의견은 활용 가능한 데이터에 의해 지지되는 것인가, 또한 검사문서는 해당 검사관이 없는 경우에도 다른 경쟁력있는 검사관이나 감독관이 무엇이 행해졌는지 평가하고 데이터를 해석하기에 충분히 상세한 것인가?

(E) 검사문서는 영속성을 지닌 것인가 또한 삭제나 지우기로부터 안전한 것인가?

(E) 다른 사람에 의해 작성된 검사문서에 근거하여 발견사항을 발행하는 사람은 관련된 검사문서의 모든 페이지를 검토하고 사건 기록에 그 검토사항을 기록하는가?

(E) 랩은 모든 증거에 대해 수행된 분석업무에 대한 보고서를 기록하고, 그 보고서는 그 분석 업무가 실행된 목적에 걸맞는 결론과 견해를 포함하는가

(E) 어디에서 결합이 이루어지는가, 결합의 정도는 명확하게 커뮤니케이션되며 적절하게 보고서에서 평가되는가?

(E) 보고서에는 작성자의 성명이 표기되는가?

- 논의 : 결합(association)의 정도, “부합하는”, “일치하는”, “일반적 출처” 등 표시를 나타내는 용어는 랩의 해석표준(interpretation)에 부합하여 보고서에서 커뮤니케이션되고 적절하게 평가되어야 한다.

(E) 랩은 검사자의 결론이 합리적이며 과학적 지식의 제한 내에 있다는 것을 보증하기 위해 보고서에 대한 기술적인 검토 시스템을 보유, 활용, 기록하는가?

논의: 기술적 검토 비율 등이 포함된 정책을 보유하고 있어야 한다. 기술 검토자는 충분한 지식을 지니고 있어야 한다.

(E) 랩은 모든 발행 보고서에 대한 행정적 검토를 수행하고 기록하는가?

(E) 랩은 각각의 검사관의 법정증언을 최소 연례적으로 모니터링하며 검사관은 평가

에 대한 피드백을 받는가?

(E) 랩이 중대한 기술적 문제가 있다는 징후가 있을 때 랩이 이를 검토하여 필요한 교정적 조치를 수행할 수 있는 절차가 기록되고 시행되고 있는가?

1.4.3. 숙련도 검사

원칙 숙련도 검사는 효과적인 품질보증 프로그램에서 필수적인 사안이다. 그것은 업무 수행을 모니터하고 향상이 필요한 부분을 알아내기 위한 많은 수단 중의 하나이다.

표준과 평가기준 각 랩은 검사관의 능력과 분석결과에 대한 신뢰성을 측정하기 위한 문서화된 숙련도 검사 프로그램을 보유하여야 한다.

(E) 랩은 문서화된 숙련도 검사 프로그램이 있는가?

논의: 숙련도 검사 프로그램은 본 매뉴얼 attachment1에 기재된 필요적 요건을 충족하여야 한다.

(E) 랩은 승인된 검사 제공자에 의해 수행되거나 승인된 제공자가 없을 경우 다른 외부의 제공자에 의해 수행되는 숙련도 검사 프로그램에 참여하는가

논의 : 랩은 연간 분야별로 최소 하나의 외부 숙련도 검사에 참여하여야 한다.

(I) 각 검사관은 사건처리가 이루어지는 각각의 하위 분야별로 매년 숙련도 검사를 받는가

- 논의 : 하위분야; 컴퓨터 포렌식, 디지털과 멀티미디어 증거 분야에서 컴퓨터 포렌식, 포렌식 오디오/비디오 분석 및 이미지 분석.

(I) 랩은 재검사 및 블라인드 기법(blind technique)을 활용한 숙련도 검사를 시행하는가?

- 논의 : 외부 숙련도 검사와 별도 (맹목기술 - 사전에 특정사건을 일반사건처럼 분석을 맡겨보는 것)

2. 개인별 적격

2.1. 경 영

○ 원칙

랩의 책임자는 가급적이면 법과학자로서의 경험을 바탕으로 과학적 기능과 랩 업무의 법과학적 측면에 대해 잘 알고 있어야 한다.

○ 표준과 평가기준

랩 책임자는 자연과학, 법과학 혹은 밀접하게 연관된 분야에 최소한 학사학위를 지니고 있어야 한다. 책임자가 과학적 배경이 부족하다면 경영에 있어 적절한 과학적 배경을 지닌 사람의 조력을 받아야 한다.

(I) 랩 책임자는 자연과학, 법과학 혹은 밀접하게 관련된 분야에 학위를 지니거나 충분히 경영자 지위와 권한을 지난 과학 관련 인사의 조력을 받는가
(D) 랩 책임자는 최소 법과학 분야에서 5년간의 경험이 있는가?
(D) 랩 책임자는 공식적인 경영에 관한 훈련을 받았는가?
(D) 랩 책임자는 최소 2년간의 경영 경험이 있는가?

(분야별 세부내용 생략)

2) 통제물질

3) 독물학

4) 미세증거

5) 생물학

6) 무기와 도구흔

7) 문서

8) 잠재지문

9) 기술지원

10) 범죄현장

11) 디지털과 멀티미디어 증거

○ 원 칙

검사관은 신뢰성 있는 결과와 결론을 만들어 내는데 필요한 이론, 절차, 기술에 대해 숙달되어야 한다.

○ 표준과 평가기준

(I) 각 검사관은 과학 분야에 대한 학사학위를 가지고 있는가?
(E) 각 검사관은 사용되는 장비, 프로그램, 방법과 절차에 대해서 이해하는가?
자격있는 검사관에 의한 지도가 끝나기 전에 독립된 사건 검사는 허용되지 않는다
(E) 각 검사관은 제공하는 검사/문서작성 혹은 증언에 상응하는 경험이 있는가?
(E) 사건 책임을 지기에 앞서 각 검사관은 자격시험을 통과하였는가?
(E) 각 검사관은 연례 숙련도 검사를 성공적으로 통과하였는가?

・논의 : 디지털과 멀티미디어 증거 검사관은 디지털과 멀티미디어 증거를 복제, 복구, 처리/보존 그리고 검사하기 위한 시스템과 절차에 대해서 알고 있어야 한다. 그들은 또한 디지털 증거 검사에서 활용되는 하드웨어와 소프트웨어에 대한 실무지식을 알고 있어야 한다. 디지털증거가 이미지들을 포함할 수 있다고 하더라도 이미지 과학과 기술의 응용은 디지털과 멀티미디어 증거분야에 제한되지 않는다,

・모든 분야에 대한 일반적 논의

신뢰성 있는 결과를 만들어내기 위해서는 적절한 개인의 자격검정이 필수적이다. 정규화된 훈련을 권한다.

어떤 분야에 대한 법과학 실행을 위한 학사 학위에 대한 요구는 학위가 필수적이지 않은 분야에 있는 누군가가 학위가 필수적인 어떠한 분야에 대해 교차 훈련(cross-train)을 받으려고 할 수 있기 때문에 면제될 수 없다.

자연과학이나 법과학이 아닌 분야에 대해 학위가 있지만 생물학과 혹은 화학에 대한 상당한 수강 경력과 수년간의 경험이 있는 자격 있는 개인들은 개별적으로 위원회의 결정에 따라 교육요건을 충족한 것으로 본다. 하지만 새로운 구성원들은 반드시 기록된 기준에 부합하여야 한다.

교육의 적격성과 별도로 훈련생들은 반드시 적절한 자격시험을 통과해야 한다. 자격시험은 현재의 연구에 대한 지식과 필기와 구술 시험, 알려진 혹은 알려지지 않은 물질에 대한 검사와 감식 및 모의 법정을 포함해야 한다.

3. 물리적 설비

3.1. 공 간

○ 원 칙

랩이 목표와 목적을 달성하기 위해 충분하고 적절한 공간이 각각의 활동과 기능에 대해 할당되어야 한다.

○ 표준과 평가기준

(I) 직원들은 할당된 작업을 수행하기에 충분한 작업 공간을 가지고 있는가?

(D) 자재창고, 장비와 도구를 위한 충분한 공간이 제공되고 있는가?

(I) 검사관을 위해 보고서를 작성하거나 다른 공식적인 커뮤니케이션을 위해 충분한 공간이 주어졌는가?

(I) 기록, 참고 자료 및 다른 필수적인 문서들을 위해 충분한 공간이 주어졌는가?

(I) 도구/장비의 동작을 원활하게 할 충분한 공간이 있는가?

(D) 도구/장비의 이용과 동작을 원활하게 할 주변장치들이 그 주변에 보관되고 있는가?

・논의 : http://www.ascld.org/pdf/library/labmgtguide.pdf 에 랩 책임자의 많은 책임들이 제시되고 있다.

많은 유가치한 참고자료들이 있겠지만 DOJ의 Forensic Laboratories:Handbook for Facility Planning, Design, construction, and Moving 참고.

3.2. 설 계

○ 원 칙

랩은 기능과 활동을 최적화되고 물리적 증거를 안전하게 보호하며 랩 운용의 기밀적 특성을 보호할 수 있어야 한다. 랩은 안전하고 건강한 작업 환경을 제공하여야 한다.

○ 표준과 평가기준

(I) 물리적 설계가 증거의 최초의 접수로부터 적절한 반출시까지 효과적인 유통을 허용하는가?

(D) 관계되는 기능적 지역의 위치가 장비와 도구의 사용을 원활하게 하는가?

(I) 부여된 임무를 수행하기에 충분하고 적절한 조명이 제공되는가?

(I) 부여된 임무를 수행하기에 적절하고 접근가능한 충분하고 적절한 배관과 배선이 있는가?

(I) 적절한 일반적인 환기시설이 있는가?

(I) 냉난방, 습기 조절이 적절한가?

3.3. 보안

○ 원칙

랩에서 보유하고 있는 물리적 증거와 기록을 안전하게 보존하는 것이 필수적이다

○ 표준과 평가기준

랩의 작업구역에 대한 출입은 통제되어야 하며 그 지역에서 정규적인 업무가 할당되거나 랩 책임자에 의해 출입이 허용된 사람에 한하여 제한되어야 한다.

(E) 작업구역에 대한 출입이 통제되고 제한되는가?

(E) 모든 외부 출입지역이 충분한 보안통제를 지니고 있는가?

(E) 제한/통제 접근이 필요한 모든 내부 구역은 잠금장치를 가지고 있는가?

(E) 모든 열쇠와 마그네틱 카드 등의 배포는 기록되고 랩 책임자에 의해 출입이 허용된 사람들에게 제한되고 있는가?

(E) 랩은 공실일 때 침입경보나 보안요원에 의해 안전한가?

(I) 랩은 화재탐지 시스템을 보유하고 있는가?

・논의 : 비상시 출입 절차에 관한 규정 필요

3.4. 건강과 안전

○ 원칙

랩은 직원들이 업무와 관련하여 부상이나 건강문제로부터 보호받을 수 있도록 건강 및 안전 프로그램을 수립하고 운영하는 것이 중요하다.

○ 표준과 평가기준

(I) 랩은 매뉴얼에 문서화된 효과적인 건강과 안전 프로그램을 보유하고 있는가?

(I) 건강 및 안전관리자로 지정된 사람이 있는가?

(I) 건강과 안전 프로그램은 정기적으로 모니터되며 요구사항을 충족하는지 연례적으로 검토되고 있는가?

(I) 랩은 특히 건강 및 안전 매뉴얼에 의해 요구되는 활용가능하고 사용할 것이 권장되는 안전장치를 보유하고 있는가?

(I) 랩은 발암물질, 독성물질 혹은 다른 위험한 물질들을 처리하기 위해 필요한 적절한 장비와 물질들을 보유하고 있는가?

(I) 랩은 안전 샤워 및 세안 장치를 적절한 위치에 보유하고 있으며 그것들은 좋은 작동상태 하에 있는가?

(I) 안전한 작업환경을 유지하기 위한 배기시설을 충분한가?

(I) 충분한 응급처방 키트가 사용가능하며 전략적으로 위치되어 있는가?

(I) 랩은 응급조치에 대한 유효한 자격이 있는 충분한 수의 인력을 보유하고 있는가?

(I) 휘발성, 가연성, 폭발성 기타 유해물질에 대한 안전한 저장공간이 충분히 제공되고 있는가?

(I) 비상시 탈출구는 충분한가?

(D) 일반적인 질서와 외관상 청결상태는 유지되고 있는가?

<부록 3>

경찰공무원의 디지털 포렌식에 대한 인식에 관한 설문 조사

최근 컴퓨터 등 디지털 증거에 대한 수사상 활용이 빈번해지고 있습니다. 이러한 디지털 증거에 대한 과학수사라고 할 수 있는 디지털 포렌식의 수요 또한 증가하고 있는 것으로 알려져 있습니다.

이 조사는 디지털 포렌식 내지 디지털 증거분석의 발전을 위한 제도변화 및 교육의 수요판단에 대한 연구를 위한 예비적 조사로, 디지털 증거에 대한 경찰수사상 활용과 관련된 경찰관의 인식을 파악하기 위해 작성된 것입니다. 바쁘시더라도 잠시 시간을 내시어 설문에 응해주시고, 조사의 익명성은 반드시 보장되오니 평소의 생각이나 행동을 그대로 답해 주시기 바랍니다.

문1. 아래 문장들에 대해 어떻게 느끼고 계신 지 해당하는 란에 √ 표시 해주시기 바랍니다.

번호	항 목	정말 그렇다	그런 편이다	그저 그렇다	그렇지 않은 편이다	전혀 그렇지 않다
1	디지털 포렌식이 무엇을 하는 것인지 알고 있다					
2	디지털 포렌식이 수사상 필요하다					
3	디지털 포렌식을 수사상 활용한 적이 있다					
4	경찰청 디지털 포렌식 센터의 존재를 알고 있다					
5	디지털 포렌식 센터에서 어떤 분석이 가능한지 알고 있다					
6	지방경찰청과 경찰서에 디지털 증거분석관의 존재 여부를 알고 있다					
7	디지털 증거분석관의 자격조건에 대해 알고 있다					
8	디지털 증거분석이 필요하지만 자체적으로 해결이 되지 않을 때 어디에 어떤 절차로 의뢰해야 하는지 알고 있다					
9	디지털 증거처리 표준 가이드라인의 존재를 알고 있다					
10	이미징(Imaging) 내지 법과학적 복제기술이 무엇인지 알고 있다					
11	디지털 매체를 어떻게 포장하여 옮겨야 하는지 알고 있다					
12	디지털 증거의 증거능력의 문제점을 알고 있다					

문2. 다음 중 디지털 포렌식의 발전을 위해서 시급한 과제는 무엇이라고 생각하시는지 세 가지만 골라 시급하다고 생각되는 순서에 따라 순위(1~3)로 표시해 주십시오

가. 충분한 전문인력의 확보 ( )
나. 교육 및 훈련 ( )
다. 법적 대응책 마련 ( )
라. 장비와 소프트웨어 ( )
마. 명확한 지침과 매뉴얼 마련 ( )
바. 기타의견 (잘 모르겠음 포함) ( )

바. 의 경우 다른 의견 _____

문3. 디지털 포렌식의 발전을 저해하는 요인이 있다면 무엇이라고 생각하는지 두 가지를 골라 더욱 심각하다고 생각되는 순서에 따라 순위(1~2)로 표시해 주십시오.

가. 예산 부족 ( )
다. 인식 부족 ( )
라. 전문성 부족 ( )
마. 지휘관의 의지 부족 ( )
바. 기타 의견 (잘 모르겠음 포함) ( )

마. 의 경우 다른 의견 _____

문4. 가장 활용도가 높은 증거분석 분야는 어떤 것이라고 생각하시는지 세 가지를 선택하여 가장 활용도가 높다고 생각되는 순서에 따라 순위(1~3)를 표시하여 주십시오.

가. 현장수사(압수수색 등) ( )
나. 컴퓨터 하드디스크 분석 ( )
다. USB 플래쉬메모리 등 이동 저장장치 분석 ( )
라. 휴대전화 기억매체 분석 ( )
마. CCTV 등 영상매체 분석 ( )
바. 오디오 분석 (디지털 성문분석 등) ( )
사. 정보통신 감시(감청) ( )

(문5~10) 질문을 읽고 해당되는 항목 번호에 ○ 표시를 해주십시오.

문5. 귀하의 경찰경력은 몇 년입니까?

가. 6년 미만 나. 6년 이상 11년 미만 다. 11년 이상 16년 미만
라. 16년 이상 20년 미만 마. 20년 이상

문6. 귀하의 근무기관은 어디입니까?

가. 경찰청(소속기관 포함) 나. 지방경찰청(소속기관 포함) 다. 경찰서
라. 지구대 마. 기타

문7. 귀하의 근무분야는 어느 분야입니까?

가. 경무 나. 생활안전 다. 경비 라. 교통 마. 수사
바. 정보 사. 보안 아. 외사 자. 기타

문8. 귀하의 직접 업무 내지 감독기능에 실제 수사업무(사건처리)가 포함되어 있습니까? (수사, 형사 및 교통사고조사, 외사・보안수사, 여청 등)

가. 그렇다 나. 아니다

문9. (문8.에서 “그렇다”로 선택한 경우에만 답해 주십시오) 귀하는 문.4에서 예시된 것과 같은 디지털 증거분석에 대한 수요가 얼마나 자주 있습니까.

가. 매우 자주 있다. 나. 가끔 있다. 다. 보통이다. 라. 별로 없다. 마. 전혀 없다.

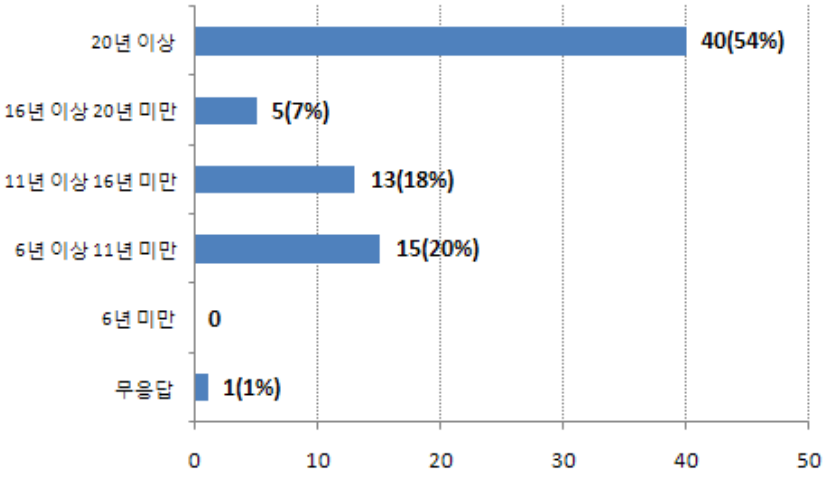
문10.(문8.에서 “그렇다”로 선택한 경우에만 답해 주십시오) 귀하는 디지털 증거분석을 위해 필요한 자원(전문인력과 장비 등)이 보강되어야 한다고 생각하십니까.

가. 매우 그렇다 나. 그렇다 다. 보통이다
라. 그렇지 않다 마. 전혀 그렇지 않다

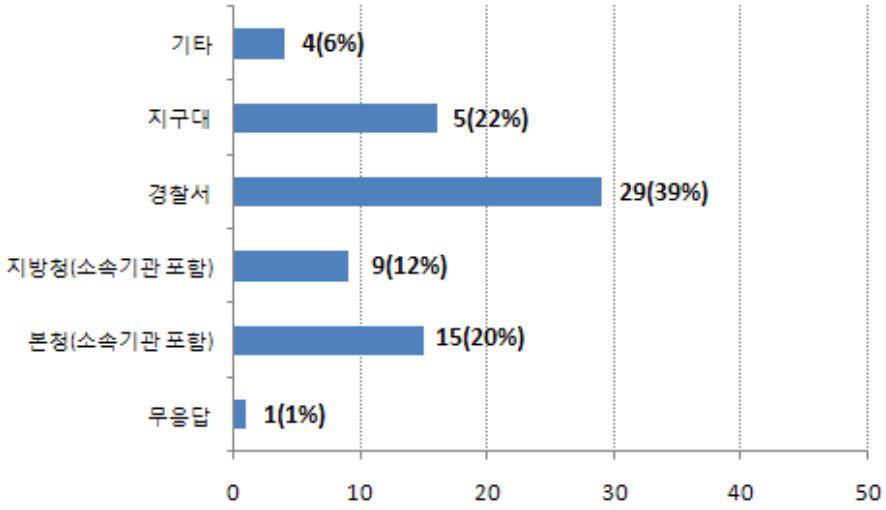
◎ 응답자 특성

❑ 연 령

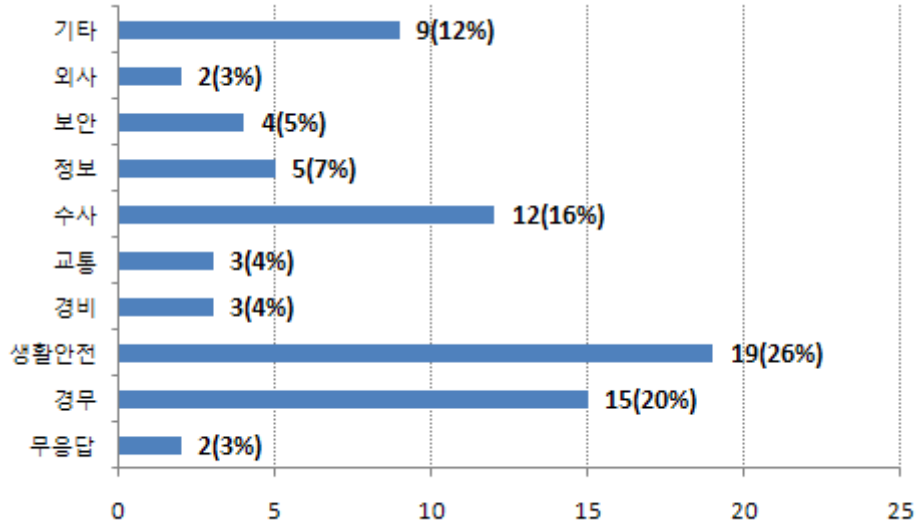
「20년 이상」이 54%로 가장 많았고, 「6년이상 11년 미만」 20%, 「11년 이상 16년 미만」 18% 순으로 나타났다.



❑ 근무지

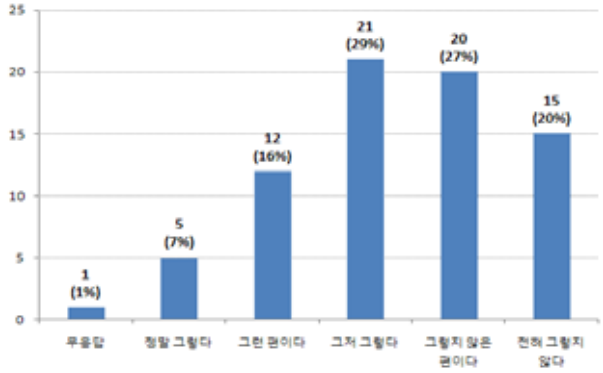


❑ 근무분야


기타
외사
보안
정보
수사
교통
경비
생활안전
경무
무응답
9(12%)
2(3%)
4(5%)
5(7%)
12(16%)
3(4%)
3(4%)
19(26%)
15(20%)
2(3%)
0
5
10
15
20
25

1. 디지털 포렌식이 무엇을 하는 것인지 알고 있다.

「그렇지 않은 편이다(27%)」, 「전혀 그렇지 않다(20%」고 응답한 비율이 47%로 디지털 포렌식에 대한 인지도가 상당히 낮은 것으로 나타났다.

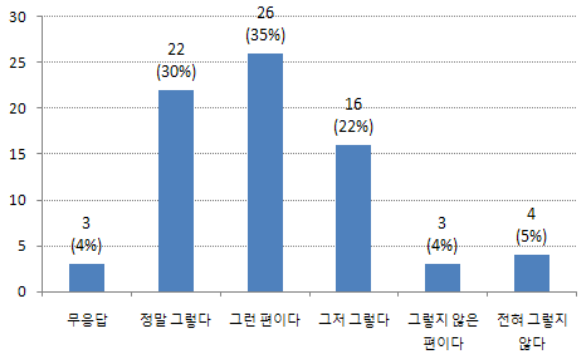


연령이 높을수록, 경찰서·지구대에 근무할수록, 경무·생활안전분야에서 근무할수록 인지도가 낮은 것으로 나타났다.

구 분		정말 그렇다	그런 편이다	그저 그렇다	그렇지 않은 편이다	전혀 그렇지 않다
근무년수	6년 미만					
	6년 이상~11년미만	1	4	5	4	1
	11년 이상~16년미만	1	3	4	3	2
	16년 이상~20년미만	0	1	0	2	1
	20년 이상	3	4	12	11	10
근무기관	경찰청	3	5	4	2	1
	지방경찰청	1	1	1	3	2
	경찰서	0	3	9	11	6
	지구대	0	2	6	3	5
	기타	1	1	1	1	0
근무분야	경무	1	3	5	4	2
	생활안전	0	2	7	5	5
	경비	0	0	0	2	1
	교통	4	1	1	0	0
	수사	1	3	3	4	1
	정보	0	0	0	2	3
	보안	2	0	2	0	0
	외사	0	0	1	0	1
	기타	0	2	2	3	1

2. 디지털 포렌식이 수사상 필요하다

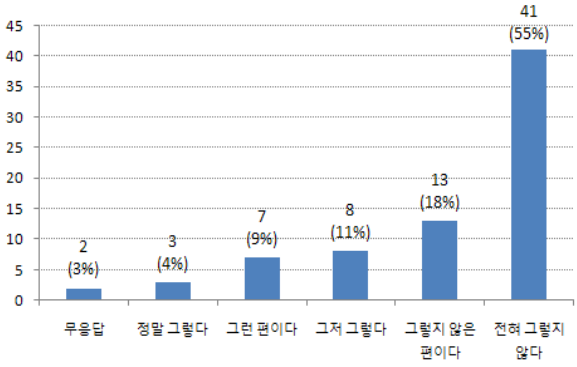
「정말 그렇다(30%)」, 「그런 편이다(35%)」고 응답한 비율이 65%로 디지털 포렌식의 필요성에 대해서는 대다수 경찰관들이 공감하고 있는 것으로 나타났다.



구 분		정말 그렇다	그런 편이다	그저 그렇다	그렇지 않은 편이다	전혀 그렇지 않다
근무년수	6년 미만					
	6년 이상~11년미만	7	6	0	0	0
	11년 이상~16년미만	4	7	1	0	1
	16년 이상~20년미만	2	1	1	1	0
	20년 이상	9	12	14	2	2
근무기관	경찰청	0	8	6	1	0
	지방경찰청	0	3	4	1	0
	경찰서	1	6	11	9	1
	지구대	1	5	5	2	2
	기타	1	0	0	3	0
근무분야	경무	1	5	4	3	1
	생활안전	1	4	8	3	2
	경비	0	1	1	1	0
	교통	0	2	1	0	0
	수사	0	5	5	2	0
	정보	0	0	2	3	0
	보안	0	2	1	1	0
	외사	1	0	1	0	0
	기타	0	3	3	2	0

3. 디지털 포렌식을 수사상 활용한 적이 있다.

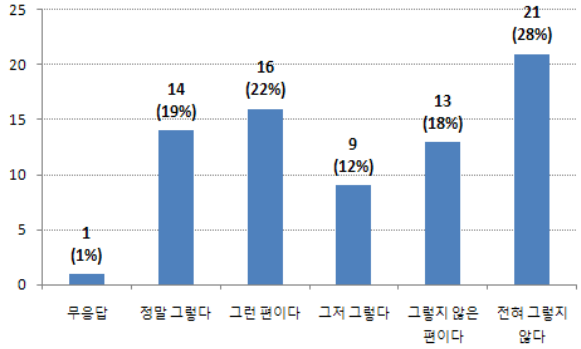
실제 수사상 활용한 경험은 「정말 그렇다(4%)」, 「그런 편이다(9%)」 등 13%에 불과한 것으로 나타났다.



구 분		정말 그렇다	그런 편이다	그저 그렇다	그렇지 않은 편이다	전혀 그렇지 않다
근무년수	6년 미만					
	6년 이상~11년미만	1	2	1	1	10
	11년 이상~16년미만	0	1	2	1	9
	16년 이상~20년미만	0	1	0	1	2
	20년 이상	2	3	5	10	19
근무기관	경찰청	1	0	2	2	10
	지방경찰청	0	2	1	1	4
	경찰서	1	3	3	6	16
	지구대	1	1	0	4	9
	기타	0	1	2	0	1
근무분야	경무	0	1	2	3	9
	생활안전	1	1	0	6	10
	경비	0	0	1	0	2
	교통	0	2	0	0	1
	수사	1	1	2	2	6
	정보	0	0	1	0	4
	보안	1	0	0	0	3
	외사	0	0	0	0	2
	기타	0	1	2	2	3

4. 경찰청 디지털 증거분석센터의 존재를 알고 있다.

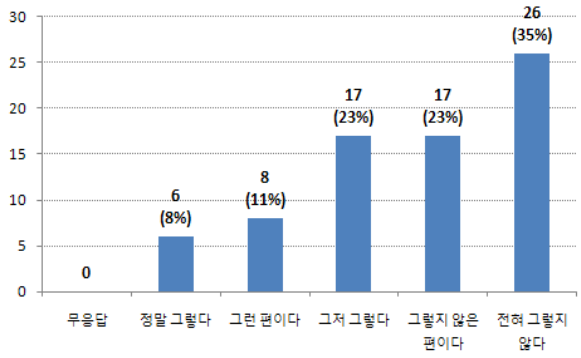
알고 있다(「정말 그렇다(19%)」, 「그런 편이다(22%)」)는 응답보다 모르고 있다(「그렇지 않은 편이다(18%)」, 「전혀 그렇지 않다(28%)」는 응답이 더 큰 것으로 나타났다.



구 분		정말 그렇다	그런 편이다	그저 그렇다	그렇지 않은 편이다	전혀 그렇지 않다
근무년수	6년 미만					
	6년 이상~11년미만	3	3	4	0	5
	11년 이상~16년미만	5	4	0	1	3
	16년 이상~20년미만	1	2	0	1	1
	20년 이상	5	7	5	11	11
근무기관	경찰청	6	5	1	1	2
	지방경찰청	1	3	1	3	1
	경찰서	6	4	5	7	7
	지구대	1	4	1	2	8
	기타	0	0	1	0	2
근무분야	경무	4	3	2	3	3
	생활안전	1	3	3	3	9
	경비	0	0	0	2	1
	교통	2	1	0	0	0
	수사	4	4	2	1	1
	정보	0	0	1	1	3
	보안	2	1	0	1	0
	외사	1	0	0	0	1
	기타	0	4	1	2	2

5. 디지털 증거분석 센터에서 어떤 분석이 가능한지 알고 있다

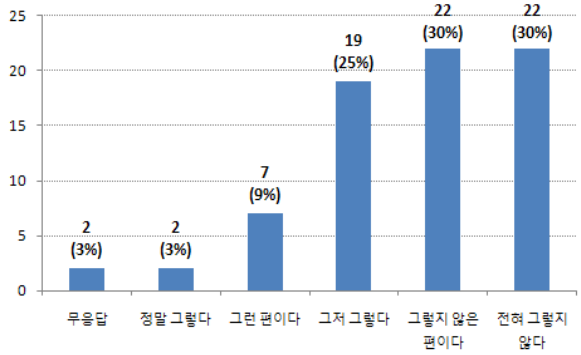
「그렇지 않은 편이다(23%)」, 「전혀 그렇지 않다(35%)」 등 과반수 이상이 디지털 증거분석 센터에서 어떤 분석이 가능한지 모르고 있는 것으로 나타났다.



구 분		정말 그렇다	그런 편이다	그저 그렇다	그렇지 않은 편이다	전혀 그렇지 않다
근무년수	6년 미만					
	6년 이상~11년미만	1	1	5	3	5
	11년 이상~16년미만	2	2	2	2	5
	16년 이상~20년미만	2	1	0	0	2
	20년 이상	1	4	10	12	13
근무기관	경찰청	3	1	6	3	2
	지방경찰청	1	2	1	3	2
	경찰서	2	3	7	6	11
	지구대	0	1	3	4	8
	기타	0	1	0	1	2
근무분야	경무	1	2	3	4	5
	생활안전	0	1	4	5	9
	경비	0	0	0	1	2
	교통	0	2	1	0	0
	수사	2	1	4	2	3
	정보	0	0	0	2	3
	보안	1	0	2	1	0
	외사	1	0	0	0	1
	기타	1	1	3	2	2

6. 지방경찰청과 경찰서에 디지털 증거분석관의 존재여부를 알고 있다.

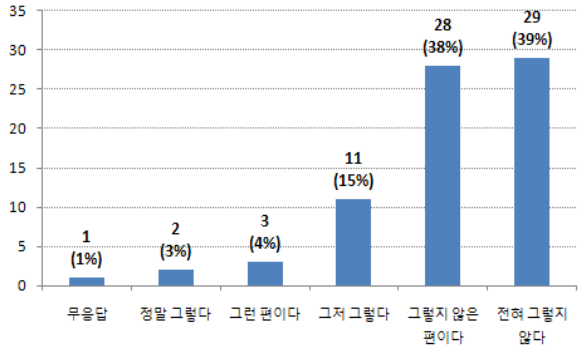
「그렇지 않은 편이다(30%)」, 「전혀 그렇지 않다(30%)」 등 과반수 이상이 지방경찰청 및 경찰서에서 근무하고 있는 「디지털 증거분석관」의 업무에 대해 모르고 있는 것으로 나타났다.



구 분		정말 그렇다	그런 편이다	그저 그렇다	그렇지 않은 편이다	전혀 그렇지 않다
근무년수	6년 미만					
	6년 이상~11년미만	1	1	3	5	5
	11년 이상~16년미만	0	2	2	5	4
	16년 이상~20년미만	0	0	2	0	2
	20년 이상	1	4	12	12	10
근무기관	경찰청	0	2	6	5	2
	지방경찰청	0	0	3	3	2
	경찰서	1	3	7	10	7
	지구대	0	2	2	4	8
	기타	1	0	1	0	2
근무분야	경무	0	1	7	4	3
	생활안전	0	2	2	6	9
	경비	0	0	0	1	2
	교통	0	1	2	0	0
	수사	1	0	3	6	1
	정보	0	0	1	1	3
	보안	0	0	3	1	0
	외사	0	0	0	1	1
	기타	0	3	1	2	2

7. 디지털 증거분석관의 자격조건에 대해 알고 있다.

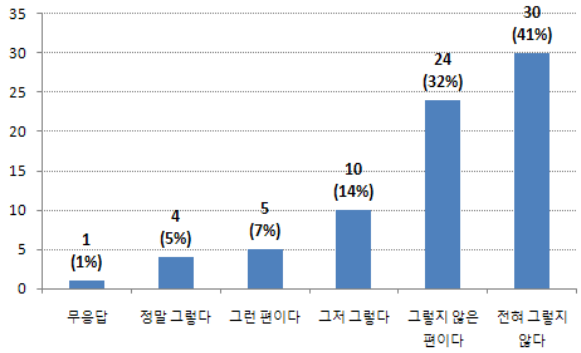
「설문 6」의 결과에서 응답자의 60%가 「디지털 증거분석관」을 모르고 있는 상태이므로, 「디지털 증거분석관의 자격조건」에 대해서는 응답자의 7%만이 알고 있는 것으로 나타났다.



구 분		정말 그렇다	그런 편이다	그저 그렇다	그렇지 않은 편이다	전혀 그렇지 않다
근무년수	6년 미만					
	6년 이상~11년미만	1	0	2	5	7
	11년 이상~16년미만	0	1	0	6	6
	16년 이상~20년미만	0	0	1	0	3
	20년 이상	1	2	8	17	12
근무기관	경찰청	0	2	3	6	4
	지방경찰청	0	0	2	4	2
	경찰서	1	0	4	11	13
	지구대	0	1	1	6	8
	기타	1	0	1	1	1
근무분야	경무	0	0	4	6	5
	생안	0	1	2	7	9
	경비	0	0	0	1	2
	교통	0	0	1	1	1
	수사	1	1	1	5	4
	정보	0	0	1	1	3
	보안	0	1	0	2	1
	외사	0	0	0	1	1
	기타	0	0	2	4	2

8. 디지털 증거분석이 필요하지만 자체적으로 해결이 되지 않을 때 어디에 어떤 절차로 의뢰해야 하는지 알고 있다.

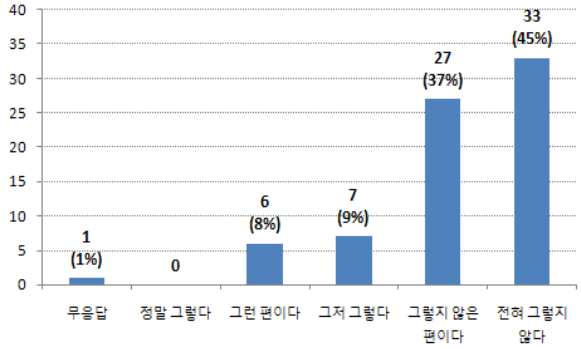
의뢰절차를 알고 있는 응답자는 12%에 불과한 것으로 나타났다.



구 분		정말 그렇다	그런 편이다	그저 그렇다	그렇지 않은 편이다	전혀 그렇지 않다
근무년수	6년 미만					
	6년 이상~11년미만	1	1	1	7	5
	11년 이상~16년미만	1	1	1	3	7
	16년 이상~20년미만	0	1	0	1	2
	20년 이상	2	2	8	13	15
근무기관	경찰청	2	2	1	5	5
	지방경찰청	0	1	1	4	2
	경찰서	1	1	5	10	12
	지구대	0	1	2	5	8
	기타	1	0	1	0	2
근무분야	경무	0	2	2	5	6
	생활안전	0	1	3	7	8
	경비	0	0	0	1	2
	교통	0	0	2	1	0
	수사	2	1	0	5	4
	정보	0	0	1	0	4
	보안	1	0	0	1	2
	외사	0	0	0	1	1
	기타	0	1	2	3	2

9. 디지털 증거처리 표준 가이드라인의 존재를 알고 있다.

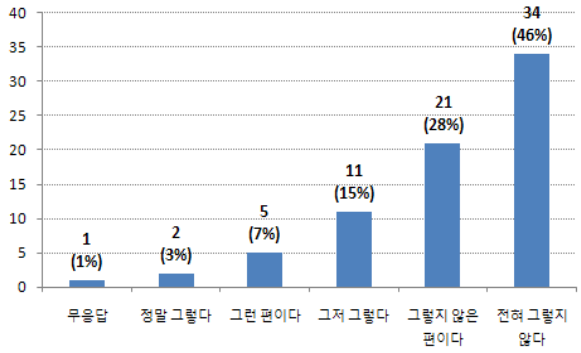
디지털 증거처리 표준 가이드라인의 존재를 알고 있다는 응답은 「그런 편이다(8%)」에 불과했다.



구 분		정말 그렇다	그런 편이다	그저 그렇다	그렇지 않은 편이다	전혀 그렇지 않다
근무년수	6년 미만					
	6년 이상~11년미만		1	1	6	7
	11년 이상~16년미만		0	1	4	8
	16년 이상~20년미만		1	0	2	1
	20년 이상		4	5	15	16
근무기관	경찰청		1	2	5	7
	지방경찰청		1	0	5	2
	경찰서		2	3	12	12
	지구대		1	1	5	9
	기타		1	1	0	2
근무분야	경무		1	2	5	7
	생활안전		1	2	7	9
	경비		0	0	2	1
	교통		0	0	3	0
	수사		1	2	5	4
	정보		0	0	1	4
	보안		1	0	1	2
	외사		0	0	0	2
	기타		1	1	3	3

10. 이미징(imaging) 내지 법과학적 복제기술이 무엇인지 알고 있다.

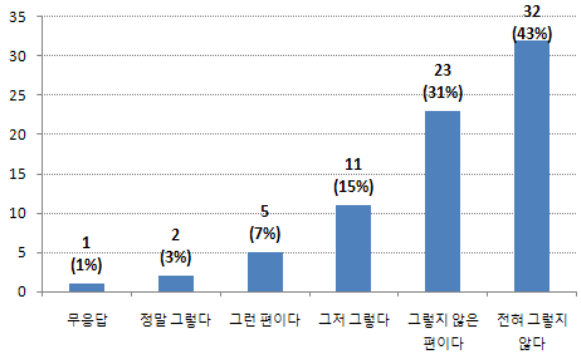
알고 있다(정말그렇다 3%, 그런 편이다 7%)는 응답 12%에 불과한 것으로 나타났다.



구 분		정말 그렇다	그런 편이다	그저 그렇다	그렇지 않은 편이다	전혀 그렇지 않다
근무년수	6년 미만					
	6년 이상~11년미만	0	1	2	2	10
	11년 이상~16년미만	0	1	2	3	7
	16년 이상~20년미만	0	1	0	2	1
	20년 이상	2	2	7	14	15
근무기관	경찰청	1	1	4	3	6
	지방경찰청	0	1	0	4	3
	경찰서	0	2	3	10	14
	지구대	0	1	3	4	8
	기타	1	0	1	0	2
근무분야	경무	0	1	5	3	6
	생활안전	0	1	4	6	8
	경비	0	0	0	2	1
	교통	0	0	0	1	2
	수사	0	2	2	2	6
	정보	0	0	0	1	4
	보안	1	0	0	2	1
	외사	0	0	0	0	2
	기타	0	1	0	4	3

11. 디지털 매체를 어떻게 포장하여 옮겨야 하는지 알고 있다.

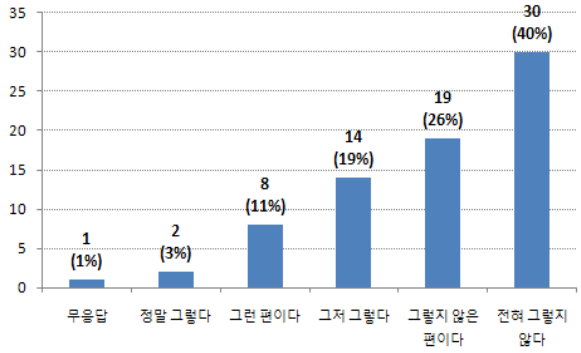
「디지털 매체를 어떻게 포장하여 옮겨야 하는지 알고 있다」는 응답이 10%에 그친 것으로 나타났다.



구 분		정말 그렇다	그런 편이다	그저 그렇다	그렇지 않은 편이다	전혀 그렇지 않다
근무년수	6년 미만					
	6년 이상~11년미만	0	1	2	6	6
	11년 이상~16년미만	0	2	1	3	7
	16년 이상~20년미만	0	1	1	2	0
	20년 이상	2	1	7	12	18
근무기관	경찰청	1	2	2	4	6
	지방경찰청	0	0	2	3	3
	경찰서	0	2	4	11	12
	지구대	0	1	2	5	8
	기타	1	0	1	0	2
근무분야	경무	0	1	4	4	6
	생안	0	1	3	8	7
	경비	0	1	0	2	0
	교통	0	0	1	2	0
	수사	0	2	1	2	7
	정보	0	0	0	1	4
	보안	1	0	0	1	2
	외사	0	0	0	0	2
	기타	0	0	2	3	3

12. 디지털 증거의 증거능력의 문제점을 알고 있다.

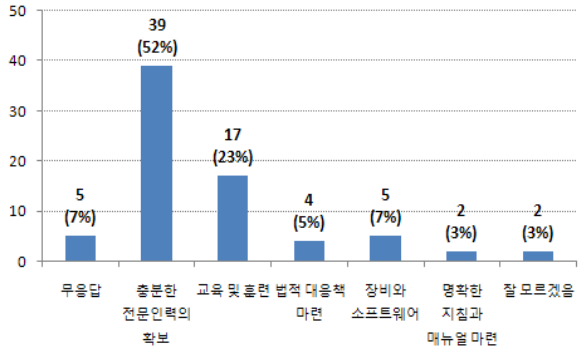
디지털 증거의 증거능력의 문제점을 알고 있는 경우가 14%에 불과한 것으로 나타났다.



구 분		정말 그렇다	그런 편이다	그저 그렇다	그렇지 않은 편이다	전혀 그렇지 않다
근무년수	6년 미만					
	6년 이상~11년미만	0	2	3	4	6
	11년 이상~16년미만	0	3	3	1	6
	16년 이상~20년미만	0	1	2	1	0
	20년 이상	2	2	6	13	17
근무기관	경찰청	1	3	2	4	5
	지방경찰청	0	0	2	3	3
	경찰서	0	4	7	7	11
	지구대	0	1	2	5	8
	기타	1	0	1	0	2
근무분야	경무	0	2	5	2	6
	생활안전	0	2	2	8	7
	경비	0	0	1	2	0
	교통	0	0	3	0	0
	수사	0	4	1	2	5
	정보	0	0	0	1	4
	보안	1	0	0	1	2
	외사	0	0	0	0	2
	기타	0	0	2	3	3

13. 디지털 포렌식 발전을 위해 가장 시급한 과제

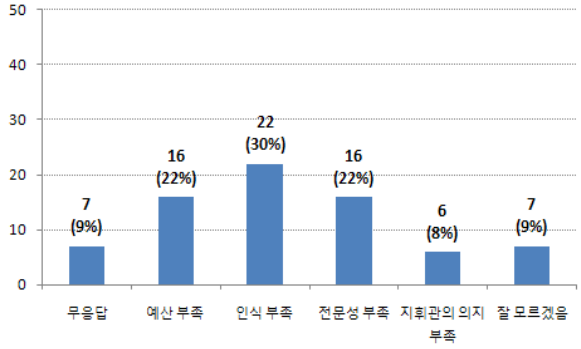
가장 시급한 과제로서 「충분한 전문인력의 확보(52%)」, 「교육 및 훈련(23%)」, 「장비와 소프트웨어(7%)」 순으로 나타나 무엇보다 전문인적자원이 확보되어 있지 않다는 인식과 이에 대한 개선필요성을 느끼고 있는 것으로 나타났다.



구 분		전문 인력확보	교육 훈련	법적 대응책	장비 소프트웨어	지침 매뉴얼	잘 모르겠음
근무년수	6년 미만						
	6년 이상~11년미만	12	1	0	1	0	0
	11년 이상~16년미만	6	1	0	3	2	0
	16년 이상~20년미만	4	0	0	1	0	0
	20년 이상	16	15	4	0	0	2
근무기관	경찰청	9	2	1	1	2	0
	지방경찰청	5	2	0	2	0	0
	경찰서	18	7	1	1	0	1
	지구대	6	5	2	1	0	1
	기타	0	1	0	0	0	0
근무분야	경무	0	2	5	2	6	6
	생활안전	0	2	2	8	7	7
	경비	0	0	1	2	0	0
	교통	0	0	3	0	0	0
	수사	0	4	1	2	5	5
	정보	0	0	0	1	4	4
	보안	1	0	0	1	2	2
	외사	0	0	0	0	2	2
	기타	0	0	2	3	3	3

14. 디지털 포렌식의 발전을 저해하는 요소

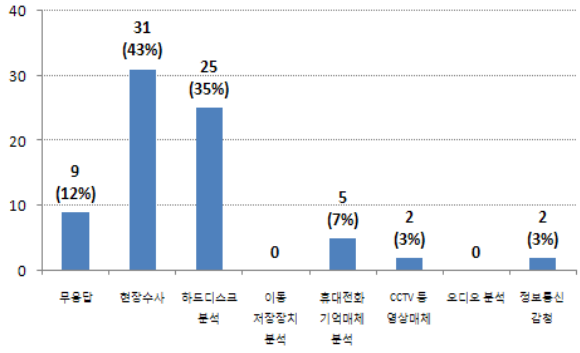
발전 저해의 가장 큰 요소로 인식부족(30%)을 들고 있다. 다음으로 「예산부족(22%)」, 「전문성 부족(22%)」순이다.



구 분		예산부족	인식부족	전문성 부족	지휘관의지 부족	잘모름
근무년수	6년 미만					
	6년 이상~11년미만	5	5	2	2	0
	11년 이상~16년미만	2	7	2	1	0
	16년 이상~20년미만	2	1	2	0	0
	20년 이상	7	9	10	3	7
근무기관	경찰청	6	3	4	2	0
	지방경찰청	3	4	1	1	0
	경찰서	6	11	7	2	2
	지구대	1	3	4	1	5
	기타	0	1	0	0	0
근무분야	경무	6	4	3	0	0
	생안	1	6	5	1	4
	경비	1	2	0	0	0
	교통	1	0	0	2	0
	수사	4	4	4	0	0
	정보	1	1	1	0	2
	보안	1	1	0	2	0
	외사	1	1	0	0	0
	기타	0	3	3	1	1

15. 가장 활용도가 높은 증거분석 분야

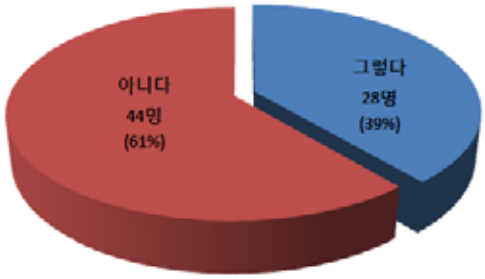
가장 활용도가 높은 증거분석 분야에 대해 응답자들은 압수수색 등 현장수사(43%), 컴퓨터 하드디스크 분석(35%), 휴대전화 기억매체 분석(7%), CCTV 등 영상매체(3%), 정보통신 감청(3%) 순으로 선택하였다.



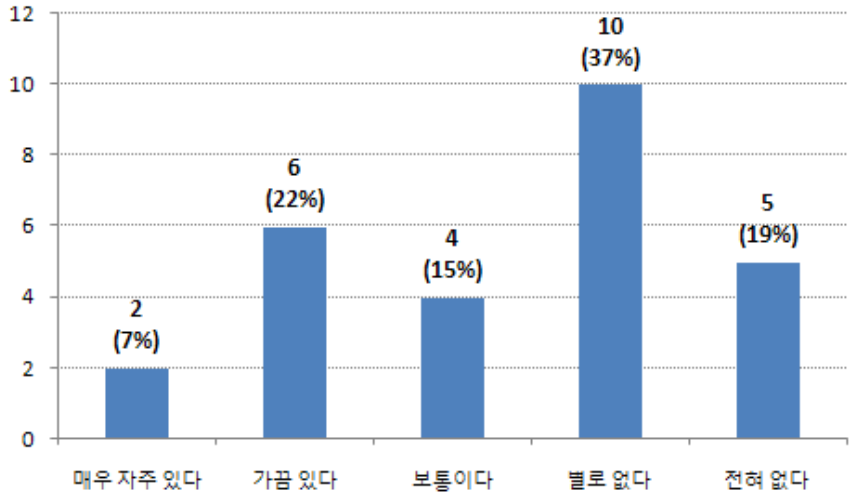
구 분		현장수사	HDD분석	휴대전화 기억매체	CCTV 영상매체	정보통신 감청
근무년수	6년 미만					
	6년 이상~11년미만	6	7	0	0	0
	11년 이상~16년미만	4	6	1	1	0
	16년 이상~20년미만	1	3	1	0	0
	20년 이상	20	9	3	1	2
근무기관	경찰청	8	6	0	1	0
	지방경찰청	3	2	1	1	1
	경찰서	10	14	1	0	1
	지구대	8	3	3	0	0
	기타	2	0	0	0	0
근무분야	경무	8	4	0	0	0
	생안	8	6	3	0	0
	경비	1	2	0	0	0
	교통	0	3	0	0	0
	수사	4	6	0	2	0
	정보	2	0	0	0	1
	보안	2	2	0	0	0
	외사	2	0	0	0	0
	기타	3	2	2	0	1

16. 직접 업무 내지 감독기능에 실제 수사업무(사건처리)가 포함되어 있는지 여부

수사, 형사 및 교통사고조사, 외사·보안수사, 여성청소년수사 등 직접 업무 내지 감독기능에 실제 수사업무(사건처리)가 포함되어 있는지 여부에 대하여 응답자의 39%(28명)가 「그렇다」라고 대답하였다.(미응답 2명)



「그렇다」라고 대답한 사람들을 대상으로 압수수색 등 현장수사, 컴퓨터 하드디스크 분석, USB 플래시메모리 등 이동 저장장치 분석 등과 같은 디지털 증거분석에 대한 수요가 얼마나 되는지를 물었다. 응답자중 8명이 「매우자주 있거나(2명, 7%)」, 「가끔 있다(6명, 22%)」고 대답하였다.



또한, 「그렇다」고 응답한 사람들중 89%가 디지털 증거분석을 위한 전문인력과 장비 등 필요한 자원이 보강되어야 한다고 생각하고 있었다.