JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 4 : 779~789 Apr. 2014

디지털 포렌식 전문인력양성 방안에 관한 연구

신준우*

A Study on Digital Forensic Human Training Method

Jun Woo Shin*

National IT Industry Promotion Agency, Daejeon 305-348, Korea

요 약

국내외 여러 대학에서 디지털 포렌식 학부과정 및 대학원 과정을 운영하고 있는데 각각 다양한 특징의 교육과정을 구성하고 있다. 본 논문에서는 새로운 학과를 만들기 보다는 기존의 IT학과와 법학과의 학생들이 4학년 학부과정에서 서로 다른 분야의 학문을 습득하도록 하는 Cross-Layer 교육과정 구성과 운영방안을 제안하였다. 먼저 디지털 포렌식 요소기술을 분석하였고, 다음으로 국내외 전문인력을 양성하기 위한 교육과정 현황을 분석하였다. 그런 다음 디지털 포렌식 전문가가 갖추어야할 수준에 대해 알아보고 IT학과 디지털 포렌식 관련 교과목 분석을 거쳐 IT+법학 교육프로그램 구성을 제안하였고 더 나아가 융합교육의 수준을 보장할 수 있는 두 가지 탄력적 교육과정 운영방안을 제안하였다.

ABSTRACT

A number of universities around the world provide various undergraduate and graduate programs for digital forensic. In this paper, we propose a cross-layer program suitable for senior students in the IT and law departments to learn multi-disciplinary convergence subjects. We have first analyzed the key ingredients of digital forensic and then the current programs in several universities. After describing the qualifications anticipated for digital forensic specialists, we have critically analyzed the courses currently offered in the IT and law departments. Based on the analysis and discussions, we have proposed an IT+law program and two flexible operation schemes of the program for securing the desired level of convergence education.

키워드 : 디지털 포렌식, 인력양성, 융합교육

Key word : digital forensic, human training, convergence education

접수일자 : 2014. 01. 10 심사완료일자 : 2014. 01. 20 게재확정일자 : 2014. 02. 10

* **Corresponding Author** Jun Woo Shin(E-mail:sjw@nipa.kr, Tel:+82-42-710-1450)
Natioanl IT Industry Promotion Agency, Daejeon 305-348, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2014.18.4.779 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

디지털 포렌식(Digital Forensic)이란 컴퓨터나 디지털 카메라, 휴대폰, CCTV, 서버 등과 같은 정보기기에 내장된 디지털 자료를 수집・복구・분석하여 발생한 어떤 행위의 사실 관계를 규명하고 증명하는 신규 보안 서비스 분야이다. 디지털 포렌식은 원래 검찰, 경찰 등의 국가 수사기관에서 범죄 수사에 활용되는 목적을 갖고 연구가 시작되었다. 그런데 정보화 사회가 급속히 발전하는 시대에서 일반 기업체 및 금융회사 등의 민간 분야에서도 활용이 증가하고 있다. 예로써, 포렌식 기술은 보험사기 및 인터넷 뱅킹 피해보상에 대한 법적 증거자료 수집, 내부 정보 유출 방지, 회계 감사 등의 내부보안 강화에 활용이 가능하다. 그런데 이와같은 중요성을 갖고 있는데도 불구하고 국내 디지털 포렌식 기술은 아직 초보단계 수준이며, 관련 전문가를 배출하기 위한 인력양성도 시작단계에 불과하다[1].

현대사회가 급속히 지식정보화 되어감에 따라 생활 전반이 첨단 IT기술에 의해 좌우되면서 사이버 범죄 등의 발생은 기하급수적으로 증가하고 있다. 이러한 환경에서 향후 디지털 포렌식 기술의 활용은 더욱 늘어날 것으로 전망되고 이에 따라 디지털 포렌식 전문가에 대한 요구는 점차적으로 증가할 것으로 예측된다[2]. 현재, 정부 조직뿐만 아니라 대기업, 중소기업 등에서도 이러한 전문가를 영입하기 위한 노력을 하고 있으나 전문인력은 크게 부족한 상황이다. 디지털 포렌식 전문가는 현재 우리나라에서 생소한 개념이고 이와 관련한 학문적 연구나 디지털 포렌식 분야에서의 법정재판 또한 운영 되고 있지 못하는 실정이다. 현재 우리나라의 수사기관에서 이를 담당하는 전문가는 디지털 기기에 대한 증거를 수색하고 추출하여 법정에 증거로 제출하는 것에 그치는 업무를 수행하고 있다. 따라서, 선진국에 준한 전문적인 교육을 받을 필요가 있다. 이러한 문제는 법학 전문가와 IT기술 전문가의 구별된 교육과 연구에 의해 나타나는 것이다.

디지털 포렌식 전문가의 경우 IT기술 측면에서 많은 연구가 이루어지고 있지만 디지털 포렌식의 가장 핵심 요소인 법정에서의 디지털 증거문제에 대해서는 다루고 있지 못하고 있다[3]. 이는 법학분야에 대한 교육 없이 오로지 기술습득에만 전념한 결과로 디지털 포렌식 분야는 규범적 시각을 바탕으로 하여 과학기술을 습득하여야 하는 것이다. 따라서 규범적 시각과 과학기술 능력을 갖춘 전문적인 인력양성이 필요하다. 즉, 압수・수색영장의 제시나 고지할 사항, 압수・수색의 범위에 관한 법적 쟁점 등을 이유로 사후 증거능력을 다투는 사례가 증가하고 있으므로, 디지털 포렌식 전문가는 컴퓨터의 기술적인 측면 이상으로 법적인 지식을 겸비하는 통합적 시각을 갖추어야 한다.

본 논문에서는 이러한 전문적인 디지털 포렌식 기술을 습득한 전문가를 양성하기 위한 IT분야와 법학분야 간의 융합교육을 통한 융합형 디지털 포렌식 인력양성을 추진할 수 있는 방안을 연구한다. 이를 위해 먼저 디지털 포렌식 전문가 요구기술을 분석하고 다음으로 국내외 디지털 포렌식 인력양성 현황을 살펴본 다음 마지막으로 디지털 포렌식 전문인력을 양성하기 위한 IT분야와 법학분야 간의 융합 교육과정 구성 및 운영방안을 제안한다. 본 논문의 구성은 2장에서는 디지털 포렌식 전문가 요구기술을 알아보고, 3장에서 국내외 디지털 포렌식 인력양성 현황을 비교 분석한다. 다음으로 4장에서는 분석한 자료를 기반으로 디지털 포렌식 전문인력 양성을 위한 IT분야와 법학분야 간의 융합 교육프로그램 구성과 탄력적 운영방안을 제안한다. 마지막으로 본 논문의 결론과 향후연구에 대하여 알아본다.

Ⅱ. 디지털 포렌식 전문가 요구기술

2.1. 디지털 포렌식 절차 및 관련기술

디지털 포렌식은 크게 증거 수집, 증거 분석, 증거 제출 절차로 이루어진다. 그림 1에 보인 바와 같이 디지털 포렌식 절차는 증거 수집을 위한 사전단계에서부터 증거 수집과 증거 분석, 데이터 복구, 결과에 대한 보고서 작성으로 이루어진다[4,5].

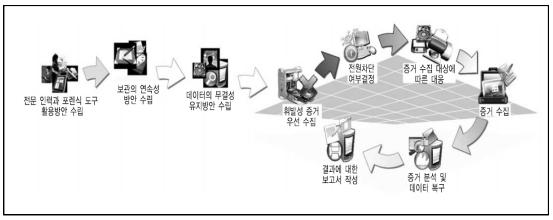

그림 1. 디지털 포렌식 절차
Fig. 1 Procedure of digital forensic

이를 증거 수집단계, 증거 분석단계, 증거 제출단계로 나누어 구체적인 절차 및 내용을 보면 아래 표 1과 같이 정리할 수 있다.

표 1. 디지털 포렌식 절차 및 기술
Table. 1 Procedure and Technique of digital forensic

항목	내용	유용한 기술
증거 수집	-손상되기 쉽고, 사라지기 쉬운 디지털 증거가 저장된 저장매체(컴퓨터 메모리, 하드디스크, USB 등)에서 데이터의 무결성을 보장하면서 데이터를 읽어 내야함 -무결성: 원 저장매체에 대한 데이터 변조가 일어나지 않음을 의미함	-무결성을 보장하는 이미징 기술
증거 분석	-증거 수집으로 얻은 데이터로부터 유용한 정보를 이끌어 내야 함 -유용한 정보는 보통 저장 매체에 존재하는 파일 시스템의 내부나 외부에 존재할 수 있음. 예를 들면, 범죄자는 저장매체에 존재하는 NTFS와 같은 파일시스템 내부나, NTFS에서 사용하지 않는 저장매체 구역에 중요 정보를 숨길 수 있음.	-삭제된 파일 복구 기술 -암호화된 파일 해독 -문자열 검색 기술
증거 제출	-압수된 디지털 증거가 법적 증거로 채택되기 위해서는 증거자료의 신뢰성이 확보되어야 함.	-법률적으로 디지털 포렌식에 대한 표준 절차 및 포렌식 툴에 대한 검증 절차

2.2. 디지털 포렌식 전문가 요구기술

디지털 포렌식 절차에 따라 증거 수집, 증거 분석, 증거 제출로 이어지는 각 단계에서 필요한 기술들을 살펴보고자 한다. 디지털 포렌식 전문가는 이러한 절차에 따른 기술들을 갖추고 있어야 한다.

2.2.1. 증거 수집

증거 수집은 대상매체의 운영체제 종료 여부에 따라서 표 2와 같이 나눌 수 있다. 포렌식 대상이 되는 라이브 시스템에서 휘발성 저장매체나 비휘발성 저장 매체에서 데이터를 획득하기 위해서는 라이브 시스템 운영체제에 있는 명령어들을 사용하기 보다는 포렌식 툴을 사용해서 데이터를 획득해야 하는데 그 이유는 세 가지로 설명할 수 있다. 첫째, 대상 시스템의 운영체제 명령들이 공격자에 의해서 이미 바뀌어 있어서 그 명령을 사용할 경우 사건 증거들을 삭제할 가능성이 있는 경우이다. 둘째, 운영체제 명령어들이 바뀌지 않았다 하더라도 정상적인 운영체제 명령의 실행이 시스템 정보를 변경할 가능성이 있는 경우이다. 셋째, 운영체제에서 제공하는 명령어들에 의해서는 접근할 수 없는 데이터나 파일들이 존재하므로 운영체제의 보호 메커니즘을 우회할 수 있는 포렌식 툴의 사용이 필요한 경우이다.

표 2. 증거 수집
Table. 2 Evidence collection

구분	내용	필요기술
데드 시스템상에서의 증거수집	-운영체제가 종료된 컴퓨터나 핸드폰 같은 기기에 대한 증거 수집 -하드디스크나 플래시 메모리로부터 데이터를 얻는 것임	-저장매체에 있는 데이터 무결성을 보장할 수 있는 이미징 기술
라이브 시스템상에서의 증거수집	-운영체제가 종료되지 않은 컴퓨터나 핸드폰 같은 기기에 대한 증거 수집 -하드디스크와 같은 비휘발성 매체 뿐만 아니라 컴퓨터 메모리와 같은 휘발성 저장 매체로부터 데이터를 얻는 것임	-라이브 시스템 운영체제에 있는 명령어를 사용하는 대신 포렌식 툴을 사용해야 함

2.2.2. 증거 분석

증거 분석은 증거 수집에서 얻어진 데이터들로부터 유용한 정보를 얻는 것을 의미하며 표 3과 같이 증거 분석 기술을 정리할 수 있다.

표 3. 증거 분석
Table. 3 Evidence analysis

구분	내용	필요기술
덤프 메모리 분석	-프로세스가 사용중인 가상 메모리의 덤프를 획득했을 경우 사용자 ID와 패스워드와 같은 유용한 정보가 남아있을 수 있음.	-프로세스가 가상 메모리를 어떻게 사용하는지를 분석해야 함
Window 레지스트리 분석	-프로그램이나 시스템에 관한 다양한 정보를 저장하고 있음. -레지스트리 Hive 파일들 중 SAM 파일은 패스워드들의 해시정보를 갖고 있으며 운영체제에 의해 암호화되고 보호되고 있음.	-SAM 파일의 패스워드를 복구해야 함
Timeline 분석	-파일 시스템은 파일생성시간과 마지막으로 접근된 시간 정보, 마지막으로 수정된 시간 정보 등을 갖고 있음.	-시간에 따른 파일 정보를 가지고 시간의 흐름에 따라 파일 생성과 접근을 알 수 있어야 함

구분	내용	필요기술
삭제된 파일복구	-파일은 여러 클러스터들의 리스트로 이루어져 있으며 이러한 리스트 정보가 파일시스템에 들어 있음. -파일을 삭제할 경우 클러스터들에 들어 있는 파일 내용을 지우는 것이 아니라 파일에 할당된 클러스터들을 프리시키는 것으로 파일을 지움	-프리된 클러스터들이 다른 파일에 할당되지 않는 한 삭제된 파일을 복구할 수 있음
비정상적 파일찾기	-사용자가 데이터를 숨길 경우에 파일을 숨김 속성으로 놓거나 파일 확장자를 바꾸어서 데이터를 숨기려 할 수 있음.	-숨김 속성을 가진 파일들이나 파일 확장자가 바뀐 파일들을 찾음
이메일 분석	-하나의 이메일을 삭제할 경우 이메일 프로그램은 메일박스에 있는 이메일의 내용을 지우는 것이 아니라 이메일의 헤더 값을 바꾸어서 삭제하게 됨	-삭제된 이메일을 복구할 가능성이 있음
로그분석	-로그는 사건 분석에 중요한 정보임. 중요한 로그들로는 파일 시스템 로그, USB사용 로그 그리고 인터넷 사용임	-사건분석에 중요한 정보가 되는 로그를 분석해야 함
슬랙 공간분석	-파일을 클러스터로 나누어 저장하게 되는데 이때 마지막 클러스터에는 파일의 가장 뒷부분을 저장한 다음 남게 되는 공간이 슬랙 공간임	-슬랙 공간에 숨겨놓은 데이터를 분석해야 함
스트링 서치	-디지털 증거 분석시 수사에 필요한 정보가 어떤 파일에 어떤 형태로 저장되어 있는지 모르는 경우가 많음 -모든 파일들을 대상으로 키워드를 가지고 검색을 반복해야 하는 경우가 많음	-대용량의 저장매체를 검색할 경우 상당한 시간이 소요되므로 검색범위를 축소하는 기술이 필요함

2.2.3. 증거 제출

증거 제출을 위해서는 디지털 증거 무결성 확보기술과 포렌식 툴에 대한 검증이 필요하다[1].

표 4. 증거 제출
Table. 4 Evidence submission

구분	내용	필요기술
무결성	-증거 자료의 신뢰성을 확보하기 위해서 수집된 데이터가 변조 및 손상되지 않았음을 해시 및 오류 검증 알고리즘을 이용하여 증명하는 기술	-법적으로 제정된 디지털 포렌식 표준 절차 및 기술이 필요
포렌식 툴 검증	-디지털 포렌식에 사용되는 포렌식 툴에 대한 인증이 꼭 필요함 -미국에서는 미국 국립표준기술연구소(NIST)에서 디지털 포렌식 툴 검증(CFTT)을 시행하고 있음	-디지털 포렌식 툴의 선정 기준을 확립해야 함 -변호사와 검사들은 디지털 증거의 객관성을 증명하기 위한 자료로 활용하고 있음

Ⅲ. 국내외 디지털 포렌식 인력양성 현황

3.1. 국외 인력양성 현황

국외의 여러 대학에서 디지털 포렌식 학부과정 및 대학원 과정을 운영하고 있는데 각각은 다양한 특징을 갖고 있다. 디지털 포렌식 교육과정 구성에 의한 체계적 운영에 많은 노력을 기울이고 있다. 미국의 경우를 보면, 여러 대학들이 학부 및 대학원 석사과정에서 디지털 포렌식 교육목표 및 비전을 정하고 이를 달성할 수 있는 교육과정을 운영하고 있는데 이를 정리하면 표 5와 같다.

이 외에도 미국의 수사기관인 National Forensic Science Technology Center(NFSTC), Federal Law Enforcement Training Center(FLETC), Regional Computer Forensics Laboratory(RCFL) 등에서 실질적인 재판준비, 증인 및 증거품과 관련한 재판준비, 디지털 포토그래피 등과 같은 사이버 범죄의 상황에 맞는 프로그램 및 기술을 습득할 수 있도록 교육과정을 개설하여 운영하고 있다[6].

또한, 영국에서도 디지털 포렌식 학사과정 및 석사과정을 여러 대학에서 운영하고 있다. 학사과정에서는 주로 사람들이 은닉한 디지털 정보를 찾는 방법과 범죄를 증명하기 위하여 데이터를 분석하는 방법을 가르쳐는데 집중하고 있다. 구체적으로 급속히 증가하는 컴퓨터 관련 범죄와 맞물려 빠르게 성장하는 컴퓨터 포렌식 분야의 커리어를 준비할 수 있도록 컴퓨터 포렌식과 IT보안의 원칙, 기술, 이론 및 적용 등에 중점을 두고 컴퓨팅의 이론과 실무를 전문적으로 교육하는 교육과정을 기반, 심화, 응용과목으로 구성된 트랙을 구축하여 운영하고 있다. 반면에 석사과정에서는 보다 심화된 과정으로 컴퓨터 보안과 관련하여 컴퓨터 범죄, 경찰작용, 증거수집의 법적 요건에 대한 지식을 쌓을 수 있도록 고

표 5. 미국 디지털 포렌식 교육현황 및 특징
Table. 5 Current Situation of Education and Feature of Digital Forensic in USA

대학	특징	
	교육목표 및 비전	교육과정
Rhode Island University 디지털 포렌식 학사과정	-컴퓨터 시스템 기본요소 또는 독립 연구 중 하나를 수강해야 함	-디지털 포렌식 1 -디지털 포렌식 분석 -범죄 또는 법에 인정되는 한 강좌 (3학점) -디지털 포렌식 2 -파일 시스템 분석 -디지털 포렌식 실습과목 -범죄와 법에 있어 추가적인 강좌
Westwood College 컴퓨터 포렌식 학사과정	-컴퓨터 포렌식, 디지털 증거 취급, 정보보안, 악성 소프트웨어 관리 분야의 전문인력양성	1. 기반과정 -기본 컴퓨터 포렌식, 멜웨어 분석 2. 심화과정 -리눅스 보안, 디스크 기반 포렌식 -모바일 포렌식, 디지털 증거 수사와 처리
Colorado State University-Pueblo 컴퓨터 정보 시스템 학사과정	-소프트웨어 및 웹 어플리케이션 개발, 시스템 분석·설계, 네트워크 설계·관리, 데이터베이스 설계·개발, IT 보안 분야에서 필수적인 지식, 기술, 능력을 개발함	<컴퓨터 정보 시스템 전공 과학 학사 과정> 1. 기반과정 -워드 & 윈도우, 파워포인트 & 웹 퍼블리싱 -엑셀 스프레드시트, 기본 웹 개발 -MS 엑세스 DBMS, 컴퓨터 정보 시스템 -PC 설계, UNIX운영 체제 2. 심화과정 -자바 프로그래밍, 심화 자바 프로그램 디자인 -네트워크 개념, 데이터베이스 -비즈니스 커뮤니케이션, 관리 원칙, 계획 관리, 응용과정, 전문 프로젝트, 세미나
Wilmington University 컴퓨터 시스템 학사과정	-컴퓨터·네트워크 보안 학사학위과정(CNS)은 학생들로 하여금 디지털 정보보안, 정보 보증, 디지털 포렌식의 전문화된 자격을 취득할 수 있도록 함	1. 기반과정 -컴퓨터 하드웨어 & 운용, 기본 리눅스 -네트워크와 텔레커뮤니케이션 -운영체제와 컴퓨터 시스템 보안 -Python 사용법, 기본 컴퓨터 포렌식 -형사사법, 정보보안의 규정과 실무 2. 심화과정 -온라인 운영체제 보안 : 웹과 데이터보안 -데이터 무결성, 컴퓨터 포렌식, 재난 복구 -네트워크 운영, 네트워크 보안 : 파이어월과 방어 -온라인 윈도우 운영체제, 온라인 리눅스 -온라인 암호학, 온라인 컴퓨터 실무가 윤리 -온라인 사이버 법률, 온라인 범죄증거와 절차
DeVry University 컴퓨터 정보 시스템 학사과정	-데브리 대학은 디지털 포렌식, 윤리, 정보 보안으로 디지털 법 적용과 절차 대처에 능숙한 전문가의 양성을 목표로 함	1. 기반과정 -디지털 범죄, 디지털 포렌식, 컴퓨터 포렌식 -기초 컴퓨터 포렌식, 기초 하이테크 범죄 -정보 보안 관련 주제, 컴퓨터 프로그래밍 -마이크로컴퓨터 하드웨어와 소프트웨어 -네트워크 기술, 운영 체제,컴퓨터 포렌식 관련 법률 2. 심화과정 -디지털 포렌식 II, 정보시스템 보안 기획과 감사 -사고 대처, 컴퓨터 포렌식 도구와 기술 -컴퓨터 포렌식 수사, 컴퓨터 포렌식 실무 -파일 시스템 포렌식 분석, 회계 포렌식 -윈도우 포렌식, 매킨토시 포렌식 분석 -컴퓨터 포렌섹 시험, 윈도우 워크 스테이션 관리 -컴퓨터 정보 보안, 정보 기술 프로젝트 관리 -컴퓨터 윤리, 정책 개선

대학	특징	
	교육목표 및 비전	교육과정
Century College 컴퓨터 포렌식 응용과학 학사과정	-컴퓨터과학, 정보보증, 컴퓨터 침해 사고, 수사, 사이버공간 윤리, 컴퓨터 관련 법률에 대하여 교육함	1. 기반과정 -윈도우 7, 마이크로소프트 윈도우 2008 서버 -리눅스 운영 체제, 컴퓨터 수사관련 법률 2. 심화과정 -컴퓨터 포렌식, 정보 보안 원칙 -오픈 소스 포렌식 방법,기본 네트워크 보안
Utica College 사이버 보안 학사과정	-최신 기술 및 데이터, 범죄학에서 사용할 수 있는 형사사법·경제범죄·컴퓨터포렌식을 통합하여 교육함	1. 기반과정 -통계, 컴퓨터 하드웨어와 주변기기, 분석 방법 -사이버크라임 수사와 포렌식 I, 범죄학 -직무 윤리, 형사사법 2. 심화과정 -사이버보안 세미나, 정보 보안 -사이버 크라임 수사와 포렌식 II, 형법의 분야 -사이버크라임 법률 3. 응용과정 -인턴쉽 -사이버크라임 수사와 포렌식 III 4. 선택과정 -컴퓨터 조직도와 프로그래밍, 수사의 현대 기술 -네트워크, 보안 관리, 정보 보안 위협, 공격 방어 -범죄 증거물, 컴퓨터와 네트워크 보안 -시스템 취약점 분석
Butler Country Community College 디지털 포렌식 학사과정	-공동체와 리더쉽을 갖추어 공동체에 도움이 되고 리더쉽이 있는 전문가를 양성하는데 중점을 둠	1. 기반과정 -컴퓨터 정보 시스템, 마이크로컴퓨팅 어플리케이션 -체력 검정, 건강 과학, C++ 프로그래밍 -PC 관리 기술, 윈도우 서버 관리 2. 심화과정 -기술적 글쓰기,데이터 커뮤니케이션과 네트워킹 -마이크로컴퓨터 운영 체제, 리눅스 -시스템 분석 & 디자인,컴퓨터와 인터넷 보안 -디지털 포렌식 I, Certification, 형법, 형사소송법 -AccessData Certified Examiner 응용과정 -네트워킹 보안, 컴퓨터 포렌식 & 보안 -디지털 포렌식 II
Champlain College 디지털 포렌식 학사과정	-디지털 포렌식의 최신 현황을 경험 -지역 수사기관과의 연계로 실무수업을 강화하고 있음	1. 기반과정 -기본 수사법, 형법 민사 사이버 크라임 수사 -기초 네트워크/보안, 공동체의 의의, Ethics -기본 포렌식 과학, 기본 컴퓨터 이론 -시스템 소프트웨어, 기본 디지털 포렌식 -Criminal Law, Law of Digital Evidence 2. 심화과정 -심화 수사법, 안티 포렌식 & 네트워크 포렌식 -디지털 포렌식 도구 평가, 모바일 포렌식 -글로벌 스터디 I : 기술 & 개발 -글로벌 스터디 II : 인권, 컴퓨터 포렌식 인턴쉽 -운영체제 포렌식, 파일 시스템 포렌식 응용과정 -E-Discovery & 데이터 분석, 고위 디지털 수사 -Investigations, 대학 최종 단계

도화된 교과과정을 운영하고 있다. 이러한 교육과정에 의해 배출된 인력에 대한 인증을 위해 EnCE 디지털 포렌식 수사자격, 미국 엑세스데이터의 FTK 포렌식전문가자격증(ACE) 자격증 등이 있다.

3.2. 국내 인력양성 현황

디지털 포렌식 분야의 전문인력 필요성이 증가함에 따라 국내 대학에서도 해당 분야의 강의를 개설하거나 학과를 만들고 있고 학원과 같은 사설교육업체에서도 디지털 포렌식 강의를 추가로 개설하고 있다. 즉, 디지털 포렌식에 대해 체계적으로 배우거나 연구를 할 수 있도록 학부나 대학원 과정이 점차 증가하고 있는 추세이다. 현재, 관련학과로는 정보보호 관련 학과가 존재하지만 아직까지는 디지털 포렌식을 전문으로 가르치는 교육체제는 부족한 편이다. 그러나, 최근 군산대, 고려대 등의 학부과정과 극동대학교, 동국대학교 대학원 등에서 포렌식을 전문으로 교육하는 학과를 개설하고 있다. 구체적인 국내 대학들의 디지털 포렌식 교육목표 및 비전과 교육과정을 정리하면 표 6과 같다[7].

한편, 이러한 교육을 통해 배출된 인력을 검증 및 인

표 6. 국내 디지털 포렌식 교육 현황 및 특징
Table. 6 Current Situation of Education and Feature of Digital Forensic

대학	특징	
	교육 목표 및 비전	교육과정
성균관대학교	-디지털 포렌식 전문가 2급 자격시험의 국가공인 자격제도에 대한 공개 교육 과정을 개설/운영함 -성균관대학교 산학협력단과 함께 공동운영 -국가기관의 공무원, 공공기관, 기업, 법무법인의 임직원은 물론 변호사 등도 참여가능	-포렌식개론(기초법률) -파일시스템과 운영체제 -개인정보보호, 컴퓨터구조 -디지털 저장 매체,데이터베이스 -응용프로그램과 네트워크 이해 -디지털 증거 분석실습 -포렌식 개론(판례동향) -디지털 증거분석 실습
고려대학교	-디지털 포렌식 전문가를 양성하기 위한 다양한 분야의 강좌를 개설함 -정보보호 관련강좌, 법학 및 범죄학 강좌, 법과학 강좌, 디지털 포렌식 기술 강좌, 디지털 포렌식 응용강좌를 개설/운영함 -우수 인력들이 최적화된 환경에서 교육을 제공함 -지능화되는 사이버 범죄에 대응할 법률, 수사, 디지털 분석 역량을 겸비한 디지털 포렌식 전문가 양성을 목표로 함	[전공필수] -정보보호기초(정보보호이론, 침해사고분석및대응) -법학 및 범죄학(사이버범죄학, 디지털증거법) -법과학(디지털법과학이론, 모의법정) -디지털 포렌식기술(디지털 포렌식기술, 포렌식랩운영) [전공선택] -정보보호기초과목(사이버법률) -디지털 포렌식응용(포렌식어카운팅, 역공학 및 악성코드분석
군산대학교	-법학과와 컴퓨터공학과가 연합하여 단순한 물리적 결합을 뛰어 넘어 학문간 융합을 통해「디지털 포렌식」교육을 실시함으로써, 오늘날 사회가 요구하는 통합적 능력을 갖춘 인재를 양성 하고 있음 -특성화를 통한 교육역량강화를 통해 통합적 능력을 갖춘 실무형 인력양성 -실무교육+법학교육+컴퓨터교육⇒디지털 포렌식	[학기별로 교과과정 운영] -디지털 포렌식개론 -컴퓨터구조와 저장매체 -디지털범죄(1), 포렌식절차법 -파일시스템과 운영체제 -디지털범죄(2),포렌식수사연습 -응용프로그램과네트워크 -포렌식 DB이해,포렌식증거법 -디지털증거분석,포렌식조사실무
대검찰청	-6개월 단위로 디지털 포렌식 전문가 양성(이론/실습:3개월, 실무훈련:3개월) -디지털 증거 압수・수색 및 분석 업무를 수행하기 위한 컴퓨터 기반의 디지털 포렌식 이론 및 실무 교육과 현장 실습 위주로 편성 -선발기준: 교육이수, 근무경력, 어학 및 컴퓨터 능력, 복무태도 등 다면 평가 -교육평가: 이론교육(1차, 2차 시험), 실무훈련(과제제출, 실무수습)	[6개월간 총 8단계] -컴퓨터/윈도우일반,리눅스 일반 -데이터베이스 일반 -디지털 포렌식 입문Ⅰ -디지털 포렌식 입문Ⅱ -파일시스템Ⅰ, 파일시스템Ⅱ -디지털 포렌식도구 사용법 -윈도우 포렌식,특수 포렌식 -사례연습, 실무훈련

증을 할 수 있는 자격증을 두고 있는데 관련 자격증으로는 한국포렌식학회에서 주관하는 디지털 포렌식전문가 자격증, 사이버포렌식전문가협회에서 인증하는 사이버포렌식조사전문가 자격증이 있다.

Ⅳ. IT분야와 법학분야 간의 융합 교육프로그램 구성 및 탄력적 운영방안 제안

4.1. 디지털 포렌식 전문가의 수준 및 IT학과 디지털 포렌식 관련 교과목 분석

디지털 포렌식은 IT기술과 법학 간의 융합학문이다. 첨단기술 및 디지털기기 등이 급속도로 발전/변화하고 있기 때문에 새로운 IT기술을 빠르게 습득해야 한다는 특징을 갖고 있다. 그리고, 디지털 자료의 분석과정은 상당한 인내를 필요로 하는 일로 사건에 따라서는 자료를 찾아 복구하고 분석하는데 많은 시간이 소요될 수도 있다. 이처럼 디지털 포렌식은 융합에 의해 새로이 나타난 분야이기 때문에 다양한 능력을 동시에 요구하며 데이터를 수집·복구하고 분석하는 과정에서는 꼼꼼하고 치밀하게 파고들어 해당 데이터를 증거력을 갖춘 자료로 만들어내야 한다. 한편, 법정에서 데이터가 증거로서 효력이 있음을 입증할 때에는 능숙하고 논리적인 언변으로 재판정에 있는 사람들을 설득할 수 있어야 한다. 디지털 포렌식 수사관이 하는 일은 크게 증거수집·복구, 증거분석, 증거 제출 등이다. 먼저 컴퓨터 메모리, 하드디스크드라이브, USB 메모리 등 저장 매체에 남아 있는 데이터를 무결하게 획득하고 수집된 데이터에서 수사에 필요한 유용한 정보를 끌어내어야 한다. 일부 데이터는 숨겨져 있을 수 있기 때문에 삭제된 파일을 복구하거나 암호화된 파일을 해독하는 등 보다 과학적인 분석기술이 필요하다.

또한, 증거분석은 복구한 데이터가 피의자의 것이 맞다는 것을 입증하는 것, 혐의사실 입증에 그 데이터가 어떤 증거능력을 가지는지 등을 명확히 제시하는 것이다. 확보한 자료는 디지털 포렌식수사관의 면밀한 분석을 통해 법정에서 효력을 발휘하는 증거로 이용하며, 법정에서 디지털 자료가 가지는 증거로서의 효력에 대해 공격이 들어오면 이를 미리 예상하고 대비할 수 있어야 한다. 마지막은 증거제출이며 이런 과정을 통해 입수된 디지털 증거가 법정 증거로 채택되기 위해서는 증거자료의 신뢰성을 확보하는 과정이 필요하다. 법률적으로 디지털 포렌식에 대한 표준절차 뿐만 아니라 증거수집 및 분석에 사용된 포렌식 툴에 대한 검증 절차도 진행된다.

디지털 포렌식은 법학, 인문학, IT기술 등의 융합으로 탄생한 분야이기 때문에 다양한 분야의 지식과 능력이 골고루 요구된다. 디저털 포렌식 전문가가 기본적으로 갖춰야할 것은 데이터 검색기술, 복구기술, 분석기술 등이며 이를 위해서는 컴퓨터시스템, 하드웨어, 운영체제, 정보보안 등 IT 전반에 대한 풍부한 지식이 필요하다. 이에 더해 논리력과 스피치 능력 등 법정에서 발휘할 수 있는 변론능력을 갖춰야 하며 글쓰기 능력도 중요하다. 디지털 자료의 확보, 복구, 해석 과정과 결과를 보고서로 작성해 법정에 제출하며 자료가 증거로 채택된 후 재판 과정에서 법리 싸움을 벌일 때에는 보고서 내용이 얼마나 논리적인지가 매우 중요하므로 이를 뒷받침하는 글쓰기 능력은 필수적이라 할 수 있다. 또한, 법적 소양도 중요하다. 특히 증거 관련 규정이 포함되어 있는 형소법이나 형법에 대한 이해가 필수적이며 앞으로 디지털 포렌식을 전문으로 하는 민간회사도 많이 나타날 것으로 예상되며 그때를 대비해 민법, 민소법에 대한 지식도 갖춰놓아야 할 것으로 보인다. 엄청난 양의 디지털 자료 중 범죄의 단서가 되는 것을 찾아내고 이것이 법정에서 증거로 채택되도록 하기 위해서는 집중력과 끈기가 필요하고, 추리력을 발휘해야 하는데 이러한 디지털 포렌식 전문인력을 양성하기 위한 체계적인 교육과정 구축이 필요한 시점이다.

본 논문에서는 이러한 디지털 포렌식 전문인력을 양성하기 위한 방안으로 IT학과와 법학과의 학부 4학년을 대상으로 한 융합 교육과정을 구성하여 학부 전문인력을 양성하기 위한 IT+법합 융복합 교육과정을 제안한다. 이는 새로이 학과를 신설하지 않고도 학부 과정에서 디지털 포렌식 인력을 양성할 수 있다는 장점을 갖고 있다. 국내 IT학과의 교육과정에서 정보보호 기술을 활용하고 있는 교과목 수를 분석해보면 대부분 교과과정에 따로 개설되어 있지 않으며 선택과목으로 2개 정도의 교과목이 개설되어 있다. 이러한 점을 감안하여 디지털 포렌식을 위한 IT분야의 교과목을 기본, 심화, 응용 수준으로 다음 표 7과 같이 정리하였다.

표 7. IT 관련학과 디지털 포렌식 관련 교과목 분석
Table. 7 Analysis of the Courses Related to the Digital Forensic in the Dept. for IT

구분	관련 교과목	분석 내용
기본	컴퓨터 구조	-디지털 포렌식을 위한 기본 IT교과목은 모든 대학의 교과과정에 이미 존재함 -디지털 포렌식의 기본 원리, IT보안의 원칙, 기술, 이론 및 적용 등을 위한 교과목이 개설되어 있지 않아 교과목 설치 및 운영이 필요함 -향후 디지털 포렌식과 보안에 관련된 핵심기술인 디지털 포렌식 원칙 및 실무 등에 관련된 교과목이 개설되어 있지 않음 -4학년 과정에 디지털 포렌식 교과목을 구축하여 선택적으로 운영함으로써 컴퓨터 시스템의 포렌식 수사와 관련 보안 분야에 흥미 있는 학생들을 교육하여 전문인력 양성의 기반을 구축할 수 있다고 판단됨
	운영체제	
	데이터베이스	
	프로그래밍	
심화	소프트웨어개발	
	정보시스템	
	컴퓨팅보안	
	네트워크와 운영체제	
응용	데이터베이스 고급	
	분산처리시스템	
	인공지능	
	프로젝트관리	

4.2. 디지털 포렌식 교육프로그램 구성

디지털 포렌식 전문가 양성을 위해 IT분야와 법학분야 간의 융합 교육과정 구성은 특화된 전문인력 배출을 목표로 교과목이 적절히 배합되어야 하고 운영방법에 있어서도 상대 학문분야에 필수적 이수를 적용시키는 Cross-Layer 이수체계를 갖추어야 함을 제안한다. 본 논문에서는 법학과 IT기술 분석에 의하여 디지털 포렌식 분야의 교과목을 편성하고자 학부 4학년 대상 융합 교육과정을 구성하였고 그에 대한 결과는 표 8과 같다.

표 8에 제시한 교육과정은 IT분야 대 법학분야의 교과목 수를 2:1의 비율로 편성하고 있음을 알 수 있다. 이는 학생이 디지털 포렌식 전문인력으로서 산업체 또는 사이버 수사를 위해 바로 쓸 수 있는 융합기술을 갖추도록 하기 위함이다. 교과목 구성은 IT분야와 법학분야의 모든 교과목이 실습이 포함된 요소설계 교과목으로 구성되어 있고, 이러한 요소설계를 병합하여 두 학문분야의 융합기술을 완성하기 위한 종합설계 교과목으로 구성되어 있다. 종합설계 교과목은 명칭이 포렌식융합종합설계프로젝트로 운영방법이 실제 사이버 범죄를 수사하는 과정에서 나타날 수 있는 상황에 따라 설계주제를 정하고 이를 해결하는 방향으로 운영됨을 알 수 있다. 종합적으로 강조하면 IT기술을 바탕으로 법학분야의 학문과 융합하는 IT+법학 융합 교육프로그램 구성은 두 학문 분야의 교과목이 적절히 배합되어야 하고 운영방법에 있어서도 요소설계 능력과 종합설계 능력을 동시에 향상시키는 메카니즘을 갖추어야 한다는 것이다.

4.3. 디지털 포렌식 교육프로그램의 탄력적 운영방안

융합교육은 두 가지 학문을 동시에 습득하게 하는 것으로 IT+법학 융합 교육프로그램을 운영하는데 있어서 특히 중요한 사항은 교육과정을 탄력적으로 운영해야 한다는 것이다. 다음은 본 논문에서 제안한 두가지 탄력적 운영방안을 보여주고 있다.

Case1: 산업체전문가 밀착 융복합교육 메카니즘

첫째는, 산업체전문가 밀착 융복합메카니즘을 들 수 있다. 표 9는 제시한 바와 같이 디지털 포렌식 기술을 습득하기 위한 독창적인 융합 메카니즘을 보여주고 있다. 즉, 요소설계교과목은 1+2+팀 체제로 운영하고 포렌식 융합종합설계프로젝트는 2+2+팀 체제로 운영한다는 것이다. 매학기 6개의 요소설계교과목에 대한 운영방식은 IT분야와 법학분야의 융합을 동시에 실현하기 위해 1(담당교수 1명) + 2(실습조교 2명:IT전문가+법률전문가) + 팀체제로 운영하는 것이고 종합설계교과목에 대한 운영방식은 설계주제를 사이버 수사상의 발생할 수 있는 범죄를 조사하는 기술과 문제해결기술을 중심으로 철저한 프로그램위원회의 심사과정을 통해 최종 주제로 선정하여 1년 동안 설계교육을 진행하는 방식이다.

표 8. 정보통신망 흐름도
Table. 8 Digital Forensic Courses for the Fourth-Year Students

학기	IT분야				실무형 융합프로젝트	법분야	
	기본원리분야		정보보호분야			포렌식기본법	포렌식절차법
2학기	파일 시스템II	응용프로그램과 네트워크	사이버 범죄 포렌식 분석 고급과정	침해사고분석 및 대응	포렌식 융합종합설계 프로젝트II	디지털 포렌식 기술 II	컴퓨터 법의학의 원칙 및 윤리적 해킹
1학기	파일 시스템I	포렌식 DB 이해	윈도우 포렌식	정보보호 이론	포렌식 융합종합설계 프로젝트I	디지털 포렌식 기술 I	디지털 증거분석

표 9. 디지털 포렌식 융합 교육과정 운영
Table. 9 Management of Digital Forensic Convergence Courses

1+2+팀 체제의 요소 설계 교과목 운영	-매학기 6개의 요소설계교과목에 대한 운영방식은 IT분야와 법학분야의 융합을 동시에 실현하기 위해 1(담당교수 1명) + 2(실습조교 2명:IT전문가+법률전문가) + 팀체제로 운영함. -먼저, 학점을 부여하는 담당교수를 산업체전문가가 담당하도록 하거나 산업체전문가가 실습조교를 담당함으로서 밀착을 융합교육을 더욱 밀착시키고 더 나아가 요소설계 주제를 법률관련 문제해결기술로 선정/추진함으로써 밀착을 강화시킨다는 것임 -다음은 융합 측면에서 보면 팀구성시 IT전공 학생과 법학전공 학생을 혼합하는 팀구성을 통해 복합학제적 팀 구성원으로서 역할과 능력을 갖추도록 하고 설계주제를 IT와 법학을 융합하는 내용으로 결정함으로서 융복합을 실현시킨다는 것임
2+2+팀 체제의 포렌식 융합종합 설계 프로젝트 운영	-매학기 1개의 종합설계교과목에 대한 운영방식은 설계주제를 사이버 수사상의 발생할 수 있는 범죄를 조사하는 기술과 문제해결기술을 중심으로 철저한 프로그램위원회의 심사과정을 통해 최종 주제로 선정하여 1년 동안 설계교육을 진행하는 방식임(주문형 설계주제 결정방식⇒탄력적 운영방식) -운영방식에서 보면 강력한 산업체 밀착과 융합교육을 실현하기 위해 2(IT전공담당교수1명+법학전공담당교수1명) + 2(실습조교2명:IT산업체전문가+법률전문가) + 팀 체제로 운영하기 때문에 아주 탄력적인 운영방식이라고 할 수 있음(산업체 밀착+융복합 추진⇒탄력적 운영방식)

Case2: Cross Layer 필수교과목 이수체계 운영

디지털 포렌식 기술을 습득하기 위해 IT전공 학생과 법학전공 학생은 3학년과정까지 배웠던 자신의 분야 외에도 서로 다른 분야의 학문을 이수해야 한다. 디지털 포렌식 기술 습득을 위해 앞서 제시한 교과목들은 서로의 분야에서 부족한 상대분야의 교과목 들을 이수해야 할 필요성이 있다. 따라서 상대 학문분야에 필수적 이수를 적용하는 Cross Layer 필수교과목 이수체계를 제안한다. IT전공 학생과 법학전공 학생이 각각 상대 전공분야에서 반드시 이수해야할 필수교과목 지정에 의한 Cross Layer 이수체계 운영방식 모델은 그림 2, 3과 같다.

IT전공 학생은 그림 2에서와 같이 법학분야의 필수요소설계교과목을 이수해야 한다. 1학기는 디지털 포렌식 개요 및 기술 등을 습득하도록 디지털 포렌식 기술 I과 디지털 증거분석을 이수하도록 지정하고 2학기는 디지털 포렌식 기술 II와 컴퓨터 법의학의 원칙 및 윤리적 해킹 등 법학에 관련된 지식을 습득하기 위해 지정하였다. 이러한 교과목 지정은 IT분야와 법학분야 교수진과의 논의를 통해 필수교과목을 선정하였는데 , 기준은 IT+법학 기술 습득을 위해 필수적으로 필요한 디지털 포렌식 관련 법학 핵심교과목이기 때문이다.

그림 2. IT전공 학생의 이수교과목
Fig. 2 Curriculum for the Students Majoring in IT

반면에, 법학전공 학생은 그림 3과 같이 IT분야 필수요소설계교과목을 이수해야 한다. 1학기는 컴퓨터 기본원리인 파일시스템I과 포렌식 DB이해 등을 필수적으로 수강하도록 하였고 그 외 윈도우 포렌식과 정보보호 이론 등은 선택으로 지정하여 학생들이 관심에 따라 기술을 습득할 수 있도록 하였다. 2학기는 파일시스템II와 응용프로그램과 네트워크를 기본적으로 수강하도록 하였고 사이버 범죄 포렌식 분석 고급과정 및 침해사고 분석 및 대응 교과목은 학생들의 선택에 의해 두 과목 중 한과목만을 선택하여 이수하도록 하였다. 결과적으로 각 분야의 전공학생은 상대분야의 교과목에서 기본 및 응용 교과목을 이수하도록 하여 디지털 포렌식 기술을 학부과정 4학년에서 최대한 습득 할 수 있도록 구성하였다.

그림 3. 법학전공 학생의 이수교과목
Fig. 3 Curriculum for the Students Majoring in Law

Ⅴ. 결론 및 향후 연구

최근 정보의 디지털화에 따른 컴퓨터 범죄의 증가에 따라 디지털 포렌식 기술은 매우 중요한 기술로 대두되고 있으며 융합에 의해 새로 나타난 분야이기 때문에 다양한 능력을 동시에 요구하는 기술이다. 이러한 디지털 포렌식 기술의 발달에 따라 디지털 포렌식 전문인력의 수요도 매우 증가되고 있는 추세이기 때문에, 디지털 포렌식 전문인력을 양성하기 위해 대학, 정부기관, 민간기관에서 많은 노력을 기울이고 있다. 이러한 취지에서 본 논문에서는 새로운 학과를 만들기 보다는 기존의 IT학과 및 법학과의 학생들이 4학년 학부과정에서 서로 다른 분야의 학문을 습득하여 디지털 포렌식 전문인력이 될 수 있는 교과과정 구성 및 운영방안을 제안하였다. 구체적으로 보면, 먼저 디지털 포렌식 요소기술을 분석하였고, 다음으로 국내외 전문인력을 양성하기 위한 교육과정 현황을 분석하였다. 그런다음 디지털 포렌식 전문가가 갖추어야할 수준에 대해 알아보고 IT학과 디지털 포렌식 관련 교과목 분석을 거쳐 IT+법학 교육프로그램 구성을 제안하였고 더 나아가 융합교육의 수준을 보장할 수 있는 두가지 탄력적 교육과정 운영방안을 제안하였다. 결과적으로 제안한 인력양성 모델을 통해 3학년까지 학생들이 자신의 전공과정을 충분히 이수하고 4학년에서 상대의 교과목을 이수하게 함으로써 보다 효율적으로 디지털 포렌식 융합기술을 습득할 수 있다고 생각한다.

감사의 글

본 연구는 2012년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2012S1A5A2A01014422)

REFERENCES

[1] I. R. Jeong, D. W. Hong, K. I. Chung, "Technologies and Trends of Digital Forensics", Electronics and Telecommunications Research Institute, *Electronics and Telecommunications Trends,* Vol. 22, No. 1, pp. 97-104, 2007. 2.

[2] J. I. Lim, "A Plan on the Next Generation Digital Forensic System of Police", Graduate School of Information, Korea University, Police Science Institute, 2007. 12.

[3] "Digital Evidence in Court: Guidelines for Law Enforcement and Inspection", Available: http://forensic.korea.ac.kr/guideline/guideline_4.pdf

[4] H. W. Lee, S. J. Lee, J. I. Lim, "Technology of Computer Forensic", *Journal of the Korea Institute of Information Security and Cryptology*, Vol. 12, No. 5, pp.8-16, 2002. 10.

[5] J. S. Kim, K. N. Kim, "Trends and Development of Computer Forensics in Korea", *Journal of Information and Security*, Vol. 3, No.1, pp. 7-22, 2003. 3.

[6] Brian Carrier, *File System Forensic Analysis*, Addison-Wesley, 2005. 3.

[7] M. S. Noh, "The development of the standard model of fit digital forensic technology education to international standards", Research Report of Ministry of Education, Science, Technology, 2012.

신준우(Jun Woo Shin)

1996년 2월 : 숭실대학교 경영학과 학사
2002년 2월 : 성균관대학교 정보통신공학과 공학석사
2010년 2월 : 고려대학교 정보관리 공학박사
1996년 2월 ∞현재 : 정보통신산업진흥원
※관심분야 : 디지털 포렌식, 인력양성, ICT R&D