# 디지털 포렌식 인력 양성을 위한 단계별 대학 교과과정 설계에 관한 연구

나현대† · 김창재†† · 이남용†††

## 요 약

사이버 공간의 지능적 범죄 증가와 예상치 않은 인터넷 대형 보안사고로 많은 물적 피해가 해마다 늘고 있는 상황이다. 이에 대형보안 사고 후 컴퓨터 범죄 수사를 위해 디지털 포렌식 기술은 필수적인 보안 분야로 자리하고 있다. 그러나 실질적으로 국내 디지털 포렌식 기술을 완비한 보안 전문 수사 인력은 미비한 편이다. 본 논문에서는 인터넷 보안사고의 과학 수사를 위한 보안 인력 양성 방안 중 하나로 대학 내 디지털 포렌식 교과 과정의 단계별 교육 과정 내용 제시하였다. 효과적인 단계별 교육 과정 제안을 위해, 현직 전문가의 인터뷰와 포커스그룹 회의 및 관련 연구를 통해 디지털 포렌식 교과 과정을 선별한 후, 이와 관련 각 과목 별 실무 적합도 및 난이도에 관한 설문조사와 인터뷰를 현직 수사관과 보안전문가를 대상으로 실시하였다. 이를 분석하여 향후 실무적응력이 높은 인력 양성을 위한 단계별 디지털 포렌식 교과 과정 설계하고 발전적인 제언과 방안을 도출하였다.

**주제어** : 디지털 포렌식, 교과 과정, 실무 적합도, 난이도, 인력 양성

# A Study on Designing an Undergraduate Curriculum in Digital Forensics per Stages for Developing Human Resource

HyeonDae Rha† · ChangJae Kim†† · NamYong Lee†††

## ABSTRACT

It is a current situation that a large number of physical and financial damages are increasing due to the growth of intellectual cyber crime and unexpected Internet incidents year by year. In the large scale security incidents, digital forensics techniques for computer crime investigations are essential to secure a place in the field. However, qualified digital forensics investigators who complete with digital security technology are practically insufficient in domestic. In this paper, as one of developing human resources plans regarding to scientific investigation of Internet security incidents, an undergraduate curriculum per stage in digital forensics was proposed. For the effective curriculum per stage, the interviews, group discussion on focused group of existing digital forensics investigators and related research were performed to select curriculum, and then the level of difficulty and practical suitability on each subject designed were analyzed through survey and interview to current investigators and security professionals. After collating the survey, the digital forensic curriculum per level was designed to highly adaptable workforce for the future for working and positive suggestions and proposals are addressed.

**Keywords** : Digital Forensics, Curriculum, Practical Suitability, Level of Difficulty, Developing Human Resource Resources

† 준 회 원: 숭실대학교 SW특성화대학원 석사과정
†† 정 회 원: 숭실대학교 SW특성화대학원 교수(교신 저자)
††† 정 회 원: 숭실대학교 SW특성화대학원 교수
논문접수: 2014년 2월 28일, 심사완료: 2014년 4월 15일, 게재확정: 2014년 5월 21일

# 1. 서론

## 1.1 연구의 필요성과 목적

정보통신망을 기반으로 한 사이버 범죄는 해킹, 바이러스, 웜의 유포를 통한 통신망의 단절 등을 비롯하여 전자 금융사기, 불법사이트 운영, 개인정보 침해 등 그 종류가 다양하고 지능화 되어 가고 있다. 경찰청 사이버 대응 센터의 유형별 사이버 범죄 건수는 2003년부터 2010년까지 지속적으로 증가하고 있어 국가적 차원에서 대책 마련이 시급히 요구되고 있다

이러한 사이버 범죄의 증가는 디지털 포렌식 기술을 필요하게 되었다. 디지털 포렌식은 디지털 소스로부터 디지털 증거를 보존, 수집, 증명, 식별, 분석, 해석, 기록, 제출하기 위하여 과학적으로 이끌어내고 증명하는 방법으로 수사관에게 디지털 증거를 수집하는 과정에서 합법적이고 과학적인 범죄 입증절차를 제시하며, 과학적인 절차에 의해 수집된 증거를 최종적으로 법원에 제출함으로써 범죄사실의 증명을 한층 강화하고 있다.

디지털 포렌식은 수사를 위한 국가 기관뿐 아니라 기업, 법무법인 등에서 소송 관련 업무에도 활용되고 있으며 근래에는 보험 조사관이나 민간 수사, 조사 업에까지 확대되어 활용하므로 그 수요가 증가하고 있는 추세이다[1]. 그러나 디지털 포렌식 전문가의 양성 기관과 관련학과의 부족으로 인해, 교육 내용이 표준화되지 못하였으며 이로 인한 정확한 교육 인재상도 정립되어 있지 않는 상태이다[2]. 또한 관련학과 이수 후 대학 4년 과정을 마친 후 실무에 투입 되었을 때 실무 적응력과 현업에서 업무 처리 능력이 저하되어 별도의 교육을 필요로 하고 있다. 그러므로 현장의 요구와 실무 적합도가 높은 교과 과정이 요구되고 있다.

## 1.2 연구 내용 및 방법

본 논문은 국내·외 관련 문헌연구를 토대로 실무 능력 배양과 국제적 표준에 부합하는 디지털 포렌식 교육을 위한 대학 내 단계별 디지털 포렌식 교과과정을 설계, 제안함을 목표로 하고 있다. 실무적합도와 난이도가 고려된 교과 과정 설계를 위해 외국 관련 문헌 연구와 현재 재직 중인 디지털 포렌식 전문가, 보안 전문가의 인터뷰, 그리고 서울지방 검찰청 디지털 포렌식 팀의 포커스 그룹 회의를 통해 대학에서 수행되어야 할 필수 과목과 기초, 선택 과목을 선별하였다. 선택된 교육 과정에 대한 실무적합도와 난이도의 검증을 위해 또다시 현업 검찰, 경찰청 수사관들과 보안 전문가를 통해 인터뷰와 설문조사를 실시하였다. 수행된 설문내용은 SPSS Statistics 버전 20을 이용하여 신뢰도, 교과 과정 실무 적합도, 난이도를 분석하였으며 각 교과별 결과값을 바탕으로 실무에 적합한 효율적인 단계별 교육과정과 현업에서 가장 많이 사용하고 있는 실습 도구와 장비, 그리고 추가적인 추천 과목, 발전 방향에 대한 제언을 하였다.

# 2. 관련 연구

## 2.1 한국

현재까지 국내 디지털 포렌식학과 라는 이름으로 별도의 학과가 존재하지 않으며, 단지 군산대 내에 디지털 포렌식 전공이라 하여 법학과와 컴퓨터정보공학과가 연합해 신설한 융복합 전공으로 재학생을 대상으로 복수전공생을 모집해 현재 16개학과 73명이 이수 중이다. 고려대학교의 정보보호대학원을 비롯하여 동국대학교, 전남대학교 등 몇몇 대학원의 정보보호 관련 학과에서 디지털 포렌식 연구를 병행하고 있다. 최근 학부과정으로는 극동대학교에서 사이버안보학과를 신설하여 디지털 포렌식 과정을 일부 교육하고 있으며 학점제 기관인 한국IT전문학교에서도 디지털 포렌식 전문 과정을 개설하여 운영하고 있다.

국내 디지털 포렌식 인력양성과 기술 교육 표준 모델을 연구한 노명선(2012)[3]의 '국제기준에 적합한 디지털 포렌식 기술교육의 표준모델 개발' 연구 논문을 참고 하였으며, 국내 디지털 포렌식 전문 인력 양성을 위한 교육 과정 개선에 관한 경기대의 김종민(2012)[4] 논문을 통해 포렌식 교육 과정 중 도구 사용법, 조사실무, 디지털 포렌식 개론, 포렌식 종류별 이론 및 개론, 시스템 포렌식의 중요도와 우선순위가 있음을 참조하였다.

### 2.2 미국

2007년 미 법무부 후원으로 West Virginia University Forensic Science Initiative에서 발행된 'Technical Working Group for Education and Training in Digital Forensics'는 미국 내 전문대학, 4년제 대학, 석,박사과정의 디지털 포렌식 교과 과정에 대한 자세한 프로그램을 소개하고 있다[5]. Champlain College는 미국 내 최초로 디지털 포렌식 학과를 개설하였으며 University of Rhode Island 는 미국무부, 국가보안처의 정보 보증 교육 분야의 우수인증을 받기도 하였다. 디지털 포렌식의 표준화를 위해 디지털 포렌식 인증위원회 (Digital Forensics Certification Board)와 국제 컴퓨터 수사 전문가 협회(IACIS; International Association of Computer Investigative Specialists)를 운영하는 점은 디지털 포렌식 교육 분야의 선진성을 보여준다. 미 국무부의 사이버 범죄센터는 사이버 수사 교육 아카데미를 운영하여 한정된 대학 내에 훈련 과정을 제공하기도 한다.

국제적 교육모델 참조를 위해 Texas A and M International University의 S. Srinivasan 'Digital Forensics Curriculum in Security Education'[6], Sam Houston State University 의 Timothy J. McGuire, Karon N. Murff 'Issues in the Development of a Digital Forensics Curriculum'[7], Champlain College의 Gary C. Kessler 'The Design of an Undergraduate Degree Program in Computer & Digital Forensics'[8]와 Dakota State University의 Manghui Tu, Kyle Cronin, Dianxiang Xu 'On the Development of Digital Forensics Curriculum'[9]이 선행 연구되었다. 대학과정 후 최종적인 미국 박사 과정의 내용을 살펴보기 위하여 California Sciences Institute의 Frederick B. Cohen, Thomas A. Johnson 'Curriculum for Digital Forensics'[10]가 참조되었다.

### 2.3 영국

University of Glamorgan의 Paula Thomas와 Iain Sutherland, University of Bristol의 Theo Tryfonas는 'An Analysis of the Curriculum Components of Computer Forensics Undergraduate Courses in the United Kingdom' 논문에서 전문가그룹의 워크숍을 통해 영국 학부 과정 중 컴퓨터 포렌식 관련 17개 학교의 교과과정을 분석하고 교육 내용을 프로그래밍, 데이터베이스, 네트워크, 개인적인 업무 능력, 포렌식 전문기술로 분류하여 각 단계별 난이도를 분석하였다[11]. 학부 과정과 연결되어 있는 디지털 포렌식 보안 대학원 과정을 참조하기 위하여 Middlesex University의 Programme Specification and Curriculum Map[12]도 참조되었다.

### 2.4 독일

2004년 처음으로 아헨공대에서 컴퓨터 포렌식 강의가 개설되었으며 만하임 대학교와 켐니즈(Chemnitz) 공대에서 컴퓨터 포렌식과 IT보안 과목이 그리고 인골스타트(Ingolstadt) 전문대학에 IT 포렌식과 IT보안 과목이 개설 되어 있다. 독일에서 디지털 포렌식 담당자가 되기 위해서는 학부를 졸업하고 디지털 포렌식 석사 과정을 졸업하거나 혹은 독일의 전문가 교육을 담당하는 민간 교육 업체에서 IT-포렌식에 대한 향상 교육을 받고 시험을 통해 담당자 증명서를 받는 경우가 있다[13].

### 2.5 대만

대만의 Tunghai University의 Hai-Cheng Chu, Kuo-Hsiung Chang과 The Overseas Chinese Institue of Technology의 Whe Dar Lin은 'Digital Forensics Core Curriculum Design in Higher Education in Ubiquitous Computing Era' 논문에서 디지털 포렌식 업무 흐름 과정을 계획, 문제 규명, 수집, 분류, 보존, 분석, 재구성, 문서화 작업, 발표의 단계로 나누고 업무 내용에 따라 각각의 분야에서 필요한 교육과정의 과목을 분석 추출하고 제시하였다[14].

## 3. 제안된 디지털 포렌식 교과과정

학부에서 디지털 포렌식 과정은 일부 관련 학과, 예를 들어 컴퓨터공학과의 상위 학년이나 포렌식 관련 유관학과에서 실시할 수 있다. 이와 달리 미국이나 영국에서는 포렌식 과정만 3, 4년 동안 배울 수 있는 독립 학과가 많이 존재한다. 향후 증가하는 사이버 범죄에 대비한 보안 인력 양성 및 수사관 인력 확충이라는 목표와 국제적 협조 수사 공조 체제 및 디지털 포렌식 학과의 국제적 상호인증을 통한 질적인 인적 자원 배양을 위해 유사한 학부 교과 과정을 운영하는 것은 의미가 있다고 본다.

### 3.1 교육목적 및 목표

디지털 포렌식 교육은 교육 대상자들에게 디지털 포렌식과 관련한 이론적 실무능력을 교육하여 차후에 발생하는 문제를 해결하여 나아갈 수 있는 능력을 가지도록 하는 것이다. 즉, 수사기관에서 디지털 포렌식 업무를 하는 사람만을 대상으로 하는 것이 아니라 디지털 포렌식 의 수요가 필요한 모든 곳에 인원의 배치가 가능하도록 신진인력의 배출이라는 것에 궁극적인 목적을 가지고 있다. 일반적인 디지털 포렌식 교육 목표는 교과 과정을 통해 아래와 같은 내용들을 습득됨을 목표로 한다.

1) 디지털 포렌식 개념의 이해
2) 증거 수집 방식의 습득
3) 증거 수집에 법률적 제한점 이해
4) 데이터 접근, 저장, 데이터 은닉 기술의 포괄적 이해와 함의성 이해
5) 다양한 저장 장치를 이용하여 데이터 회복 기술 습득과 차이점 이해
6) 포렌식 관련 법률 이해
7) 디지털 포렌식 관련한 윤리적 문제에 대한 분석과 이해

### 3.2 교과 과정

각 선행연구에서 보이는 제안 교과 과정은 차이점이 있으나 각 논문에서 추천하는 과목들의 공통적 요소를 선별하고 중복되는 과목을 분류하여 종합적으로 아래와 같이 필수 과목과 선택 과목으로 학부 디지털 포렌식 교과 과정을 제안 하였다. 필수 과목은 디지털 포렌식 분야의 내용을 포함하는 필수 전공과목의 형태이며, 선택 과목은 필수 과목을 이수하기 위한 선수 과목, 즉 사전 배경 지식으로 필요한 과목을 선별하였다.

위의 과정들을 분석해 보았을 때 기본적인 디지털 포렌식 과정의 기술적 측면과 법률 관련한 내용이 조화를 이루며 실습을 위한 프로젝트나 법원 경험, 인턴 과정을 적절히 배합하여 실무 능력을 향상시키는 교과 과정을 운영해야 할 것으로 판단된다.

효율적인 디지털 포렌식 교육을 위해 도구의 실습과 이를 위한 전용 실습 환경은 필수적인 요소다. 미국 대학과 같이 데이터 복구(Recovery) 실습실, 네트워크 보안 실습실, 사이버전쟁 시뮬레이션 실습, 디지털 포렌식 검사실을 두고 실습 환경을 마련하는 것도 실무 적응력을 높이는 대안이 될 수 있다.

데이터 원복 실습실의 경우 하드 드라이브 재프로그래밍 장비와 툴을 보유하여 하드 디스크 불량과 트랙, 펌웨어, RAID 데이터 분실에 관한 실습을 교육하도록 한다. 네트워크 보안 실습실에서는 데이터, 네트워크 보안 뿐 아니라 사이버 보안 침임 탐지에 관한 내용을 교육하며, 실습실 환경도 3개의 실제 분리된 네트워크 환경을 구성하여 각 네트워크에는 서버, 방화벽, 라우팅, 스위치 장비를 무선으로 접속이 가능하도록 한다. 모든 네트워크 하드웨어 장비는 고성능 급의 라우터, 스위치, 방화벽, 무선 AP, 고성능 서버로 구성하고 네트워크 분석 장비를 활용 하여 네트워크 트래픽과 이벤트를 모니터 하고 추적하는 활동, 네트워크 하드웨어, 소프트웨어의 오류를 수정 하는 실습을 수행하도록 한다. 사이버 전쟁에 대비하여 모의 가상훈련으로 시뮬레이션 실습을 수행하며 수사전용 검사실을 두어 디지털 포렌식 실습을 훈련한다.

관련 문헌 연구와 현직 디지털 포렌식 전문가와 보안 전문가의 인터뷰, 그룹 회의를 통해 제안하는 교과 과정 목록은 아래 <표 1>과 같다.

<표 1> 제안 교과 과정 목록

| 분류 | 과목 명 | 설 명 |
|---|---|---|
| 필수 과목 | 디지털 포렌식 개론 | 디지털 포렌식 조사 절차, 규정, 법률에 대한 내용을 다루며, Encase, FTK와 같은 기본적인 오픈, 상용 포렌식 툴을 다룸. 증거 수집, 보존, 분석, 보고, 발표에 관한 총론을 학습함. |
| | 고급 디지털 포렌식 | 포렌식의 고급 과정으로 암, 복호화와 윈도우 레지스트리, 메모리 분석 고급 파일 시스템 분석, 삭제 은닉 데이터, 메타데이타, 익명/실행 파일 분석, 응용, 복호화에 관한 내용을 학습 함. |
| | 네트워크/인터넷 포렌식 | 인터넷, 네트워크 보안, 윤리적 해킹, 네트워크 트래픽 분석, 로그 분석, 웹 공격, DOS/D-DOS조사, 이메일 포렌식, 인터넷 애플리케이션 포렌식, 소셜 컴퓨팅 포렌식(social networks/Web2.0), 악성코드 분석에 관해 학습함. |
| | 모바일 포렌식 | 무선 보안 공격, 무선 트래픽 조사, 스마트폰 관련한 포렌식을 학습함. |
| | 시스템 포렌식 | 시스템 관련 포렌식으로 악성코드, 임시 파일 분석 및 전자 증거물 등을 사법기관에 제출하기 위해 과학적 증거 수집 및 분석기법의 일종으로, 이 메일 접속기록 등의 정보를 수집, 분석하여 범행과 관련된 증거를 확보하는 기법에 관해 학습 함. |
| | 데이터베이스 포렌식 | 데이터(회계, 이메일, 전자결재, 업무용 데이터베이스)의 분석 및 삭제, 갱신된 내용을 복원하는 등 데이터베이스 포렌식에 관해 학습함. |
| | 안티포렌식 기술 | 안티포렌식 개념과 방법에 관해 학습함. |
| | 역공학 (Reverse Engineering) | 기존의 시스템으로부터 문서 또는 설계기법의 데이터를 역으로 얻어내는 역 공학(Reverse Engineering)에 대해 학습함. |
| | 암호분석 실무 | 암호화된 데이터나 자료를 해독하는 기술을 학습함. |
| | 이미지 방법과 저장 기술 | 디지털 자료 중 하나인 이미지 데이터의 처리 방법과 저장 기술을 습득하여 증거 자료로서 활용을 학습함. |
| | 디지털 포렌식 관련 윤리 | 디지털 포렌식 관련한 다각적인 인권과 윤리의 문제를 학습함. |
| | 형사 절차 및 범죄 수사 실무 | 형사소송법의 이론을 형사절차의 진행순서로 체계화하고 최신 판례와 주요 서식, 결정문 작성 예를 정리하며, 형사소송법 전반에 관하여 쉽게 이해하여 수사업무 및 송치서류 작성법 등, 유형별 수사 방법과 실무에 관해 학습함. |
| | 정보통신망 법 | 정보통신망 법에 대한 개념과 전반적인 내용을 배워 실무에 적용함. |
| | 개인정보보호법 | 개인정보보호법에 대한 개념과 전반적인 내용을 배워 실무에 적용함. |
| | 정보통신기반 보호법 | 정보통신기반 보호법에 대한 개념과 전반적인 내용을 배워 실무에 적용함. |
| | 포렌식 도구 실무 실습 | 이론의 적용을 위해 실습환경에서 포렌식 툴의 사용법과 적용을 실습함. |
| | 디지털 포렌식 프로젝트 실습 | 디지털 포렌식 지식과 기술을 활용하여 사이버 범죄에 관한 연구 프로젝트를 수행함. |
| | 법정 실습 및 인턴 | 공공, 사설 분야에 실습생으로 실무 경험을 습득하고, 모의 법정 체험 과정을 통해 실제 시나리오 시뮬레이션에 참여하여 학생들은 배운 것을 적용하고 법정 경험을 얻고자 함. |
| 선택 과목 | 암호학 | 정보 보호 기반 기술의 이해를 돕기 위해 암호학의 이론적 배경과 동작 원리를 배우며, 안티 포렌식 기술 중 하나인 스테가노그라피(정보은닉기술)를 배움으로 기밀 정보가 이미지 파일이나 MP3 파일 등에 암호화되어 있는지 파악할 수 있음. |
| | 컴퓨터, 데이터 통신 | 데이터 통신의 기본 원리를 다루어 네트워크의 이해를 목적으로 함. |
| | 정보 보안 개론 | 기본 정보 보안 과목임. |
| | 컴퓨터, 네트워크 보안 | 보안 영역 중 컴퓨터, 네트워크 보안 분야를 중점적으로 학습함. |
| | 운영체계 | 운영체제 이해를 위한 기본적인 프로세서 중심의 컴퓨터 시스템 개요와 운영체제의 전반적인 내용과 프로세스, 메모리, 장치(디스크) 파일, 분산처리, 보안등을 학습 함. |
| | 민사, 형사 소송법 | 민사, 형사 소송법의 대한 법률적 이해를 목표로 함. |
| | 데이터베이스 실무 | 데이터베이스 기본개념 및 설계 기법과 실무 적용에 관해 학습함. |
| | 수사 인터뷰 기법 | 범죄 수사학에 근거하여 수사 인터뷰의 원칙, 기법, 절차, 방법에 관해 학습함. |
| | 증거 수집법 | 과학적인 증거에 대한 기본법리를 설명하고 과학적 증거에 접근하는 방법론에 관해 학습함. |
| | 그래픽 파일의 복구 | 그래픽 파일의 백업, 삭제, 복구 관련 기술을 학습함. |
| | 침해사고 대응실습 | 침해 대응 실무 및 구축 방법에 대한 학습함. |
| | 소프트웨어 공학 | UML, JAVA등 프로그래밍과 소프트웨어의 개발, 운용, 유지보수, 요구 공학, 테스트 등 생 |

| | | |
|---|---|---|
| | | 명주기 전반을 체계적으로 학습함. |

# 4. 디지털 포렌식 교과 과정 설계에 관한 검증

## 4.1 설문과 인터뷰 시행

현재 서울 지방 검찰청과 경찰청 사이버 테러 대응 센타에서 디지털 포렌식 종사 관련자와 한국인터넷 진흥원의 보안전문가, 한국지역정보개발원의 보안 업무 종사자등 52명을 대상으로 제안된 교과 과정에 대한 실무 적합도와 난이도를 5단계로 분류하여 설문조사와 인터뷰를 시행하였다.

설문에 대한 신뢰도는 <표 2>와 같다

<표 2> 교과과정 실무 적합도와 난이도 설문의 신뢰도

| 디지털 포렌식 과목 | 실무적합도의 신뢰도 Cronbach의 알파 값 | 난이도의 신뢰도 Cronbach의 알파 값 |
|---|---|---|
| 18개 필수과목 | 0.858 | 0.848 |
| 12개 선택과목 | 0.809 | 0.802 |

Cronbach의 알파 값을 검토 하였을때 모두 0.8 이상 나옴으로써 설문에 대한 신뢰도가 높음을 보여주고 있다.

## 4.2 검증 결과

논문에서 적용한 검증에 대한 분야별 결과는 다음과 같다.

### 4.2.1 교과 과정의 실무 적합도

교과 과정별 실무 적합도는 <표 3>과 같이 통계 집계 되었다.

<표 3> 교과 과정별 실무 적합도

| 과목 명 | 평균 | 표준 편차 |
|---|---|---|
| 디지털 포렌식 개론 | 4.23 | .877 |
| 고급 디지털 포렌식 | 4.27 | .843 |
| 네트워크/인터넷 포렌식 | 3.90 | .975 |
| 모바일 포렌식 | 3.73 | .992 |
| 시스템 포렌식 | 4.06 | .850 |
| 데이터베이스 포렌식 | 3.85 | .916 |
| 안티포렌식 기술 | 3.33 | .901 |
| 역공학(Reverse Engineering) | 3.81 | 1.138 |
| 암호분석 실무 | 3.31 | 1.076 |
| 이미지 방법과 저장 기술 | 3.67 | 1.004 |
| 디지털 포렌식 관련 윤리 | 3.40 | 1.089 |
| 형사 절차 및 범죄 수사 실무 | 3.92 | .967 |
| 정보통신망 법 | 3.62 | .953 |
| 개인정보보호법 | 3.69 | .940 |
| 정보통신기반 보호법 | 3.71 | .957 |
| 포렌식 도구 실무 실습 | 4.19 | .886 |
| 디지털 포렌식 프로젝트 실습 | 3.65 | .947 |
| 법정 실습 및 인턴 | 3.37 | 1.048 |
| 암호학 | 3.33 | .901 |
| 컴퓨터, 데이터 통신 | 3.60 | .975 |
| 정보 보안 개론 | 3.62 | .953 |
| 컴퓨터, 네트워크 보안 | 3.77 | .962 |
| 운영체계 | 3.88 | .943 |
| 민사, 형사 소송법 | 3.29 | .825 |
| 데이터베이스 실무 | 3.56 | 1.018 |
| 수사 인터뷰 기법 | 3.29 | 1.126 |
| 증거 수집 법 | 3.67 | 1.061 |
| 그래픽 파일의 복구 | 3.23 | .942 |
| 침해사고 대응실습 | 3.73 | 1.087 |
| 소프트웨어 공학 | 2.79 | .936 |

### 4.2.2 교과 과정의 난이도

교과 과정별 난이도는 <표 4>과 같이 통계 집계 되었다.

<표 4> 교과 과정별 난이도

| 과목 명 | 평균 | 표준 편차 |
|---|---|---|
| 디지털 포렌식 개론 | 2.83 | .810 |
| 고급 디지털 포렌식 | 4.02 | .804 |
| 네트워크/인터넷 포렌식 | 3.63 | .817 |
| 모바일 포렌식 | 3.44 | .826 |
| 시스템 포렌식 | 3.77 | .807 |
| 데이터베이스 포렌식 | 3.85 | .978 |
| 안티포렌식 기술 | 3.42 | .915 |
| 역공학(Reverse Engineering) | 4.00 | 1.048 |
| 암호분석 실무 | 4.08 | 1.064 |
| 이미지 방법과 저장 기술 | 3.12 | .963 |
| 디지털 포렌식 관련 윤리 | 2.58 | 1.036 |
| 형사 절차 및 범죄 수사 실무 | 3.00 | .886 |
| 정보통신망 법 | 2.81 | .687 |
| 개인정보보호법 | 2.92 | .788 |
| 정보통신기반 보호법 | 2.83 | .785 |
| 포렌식 도구 실무 실습 | 3.17 | .834 |
| 디지털 포렌식 프로젝트 실습 | 3.48 | .852 |
| 법정 실습 및 인턴 | 3.00 | .886 |
| 암호학 | 3.75 | .968 |
| 컴퓨터, 데이터 통신 | 3.35 | .905 |
| 정보 보안 개론 | 2.94 | .938 |
| 컴퓨터, 네트워크 보안 | 3.23 | .757 |
| 운영체계 | 3.50 | .780 |
| 민사, 형사 소송법 | 3.30 | .863 |
| 데이터베이스 실무 | 3.31 | .805 |
| 수사 인터뷰 기법 | 3.15 | .849 |
| 증거 수집 법 | 3.04 | .713 |
| 그래픽 파일의 복구 | 3.19 | .817 |
| 침해사고 대응실습 | 3.52 | .828 |
| 소프트웨어 공학 | 3.21 | .893 |

#### 4.2.3 실무적합도, 난이도별 상위 5개 과목

실무 적합도와 난이도가 높은 상위 5개 교과과정은 <표 5>와 <표 6>과 같다.

<표 5> 실무적합도 상위 5개 과목 명

| 순위 | 교과 과정 명 | 실무적합도 | 표준편차 |
|---|---|---|---|
| 1 | 고급 디지털 포렌식 | 4.27 | .843 |
| 2 | 디지털 포렌식 개론 | 4.23 | .877 |
| 3 | 포렌식 도구 실무 실습 | 4.19 | .886 |
| 4 | 시스템 포렌식 | 4.06 | .850 |
| 5 | 네트워크/인터넷 포렌식 | 3.09 | .975 |

<표 6> 난이도 상위 5개 과목 명

| 순위 | 교과 과정 명 | 난이도 | 표준편차 |
|---|---|---|---|
| 1 | 암호 분석 실무 | 4.08 | 1.048 |
| 2 | 고급 디지털 포렌식 | 4.02 | .804 |
| 3 | 역공학(Reverse Engineering) | 4.00 | 1.048 |
| 4 | 데이터베이스 포렌식 | 3.85 | .978 |
| 5 | 시스템 포렌식 | 3.77 | .807 |

#### 4.2.4 설문지외 추가 추천 교과 과정

위의 설문지에서 제공하는 필수과목과 선택 과목 외에 추천할 교과 과정을 묻는 질문에 응답자들은 아래 <표 7> 과 같은 과목을 추천하였다.

<표 7> 설문 외 추천 교과과정

| 과목 명 |
|---|
| 클라우드 및 가상화 컴퓨팅 |
| 클라우드와 빅데이터 |
| MAC Time연구 |
| 클라우드 포렌식 |
| 실무포렌식 사례연구 |
| Encase실습 |
| C, Java, Assembly등 프로그래밍 과목 |
| SW개발 실습 |

위의 내용을 살펴 볼 때 최근 많이 사용하는 클라우드 환경에 대비한 포렌식에 대한 요구가 필요하며 최신 이슈인 빅데이터에 대한 과정을 추천하였다. 또한 실무 내용이 중요함에 따라 다양한 사례 연구와 실습, 소프트웨어의 프로그래밍과 개발 실습이 차후 분석 업무에 도움이 됨을 보여 주었다.

### 4.3 디지털 포렌식 활용 도구 및 실습 환경

디지털 포렌식 수사를 위해 사용하는 도구나 장비에 관한 설문 조사에서 가장 많이 사용하는 것은 Encase와 FTK이며, 요즘 대두되는 모바일 포렌직을 위해서는 XRY, CellBrite, Oxygen, BitPim, TULP2G를, 미디어 포렌식을 위해서는 VideoFOCUS, dTective, ClearID DAC, Magnifi Spotlight 도구를 활용함을 보여주었다. 향후 허니팟(honeypot)을 설치하여 네트워크 포렌식 수사 기법을 실습하고 악성 코드 및 Facebook, MySpace, Twitter, Blogosphere와 같은 소셜 컴퓨팅 포렌식 분석을 위해 정확한 수사 기법의 툴을 실습하도록 한다. 설문조사 결과 수사를 위해 가장 많이 사용하거나 추천하는 도구나 장비의 목록은 아래 <표 8>과 같다.

<표 8> 수사를 위해 가장 많이 사용하거나 추천하는 도구와 실습 장비

| 도구 명 | 설명 |
|---|---|
| Encase | Guidance Software사 제품, 디지털 포렌식 분석도구로 가장 많이 쓰이고 있음. |
| FTK(Forensic Took Kit) | Access Data사 제품, 포렌식 수사에 필수적으로 사용하며 FTK제품을 설치하여 숨겨진 파일이나 삭제 파일을 찾을 수 있음. 교육용 데모버전을 무료로 제공함. |
| Imagemaster Solo | 복제 장비로, 복제 시 무결성 입증을 위한 알고리즘 제공. |
| Final Forensic | Encase와 유사한 포렌식 통합 분석도구로 복구에 좀 더 초점이 맞추어짐. |
| CFT | 디지털 증거수집도구로 검찰청과 국가보안연구소에서 사용 중임. |
| Tableau | 쓰기 방지 장치임. |
| Wireshark | 네트워크 패킷 캡쳐 및 분석 툴, 패킷 스니핑 도구임. |
| XRY | Mico Systemation사가 만들 모바일 디지털 장비 분석을 위한 포렌식 시스템임. |
| Fastblock | Giudance사의 제품으로 하드디스크등 디지털 분석을 위한 원본 변경을 막는 쓰기 방지 장치임. |
| RoadMASSter3 | 이동형 포렌식 장비로 디지털 증거 수집,, 복제, 삭제 및 분석을 위해 사용됨. |
| Volatility | 메모리 분석 도구임. |
| Ollydbg | 윈도우용 2진 파일 분석기, X86디버거임. |
| Regshot | 실시간 레지스트리 변경 확인 프로그램임. |
| IDA pro | 악성코드분석과 리버싱을 위해 사용됨. |
| Sysinternals Suite | 윈도우용 유틸리티로 리버싱을 위해 사용됨. |

| | |
|---|---|
| Log explorer | 데이터베이스 포렌식 도구 |
| Intella | 이메일을 전문적으로 분석하는 도구 |
| i2 | IBM에서 제공하는 수사용 분석 도구 |

### 4.4 교과 과정을 위한 실무자로서의 조언

주관식으로 실시한 디지털 포렌식 교과 과정 설계 시 실무자의 조언과 제언을 묻는 질문에 응답자들은 아래 <표 9>와 같은 의견을 제시하였다. 실무 위주의 현장 연계성 있는 교과 과정을 수립하며 정확한 이론과 IT정보 기술의 이해의 토대 위에 포렌식 교과 과정이 설계되어야 함을 보여주었다.

<표 9> 교과 과정을 위한 실무자로서의 조언

| 조언 및 제안 내용 |
|---|
| 기초에 중점을 둔 깊이 있는 교과 과정의 교육 추천 |
| 이론보다는 실습, 사례 위주의 교육 과정 |
| 특정업체 소프트웨어 사용 및 운영지양 |
| 실무위주, 실무연계 교육 |
| 안티 포렌식에 대한 대응 학습 |
| 모바일 포렌식의 중요성 |
| IT전반적인 시각을 키울 수 있는 과정 설계 이루어져야 함 |
| 절차의 중요성과 증거 무결성 강조한 교과과정 |
| 실제 포렌식 수사를 했던 사례를 수집하여 포렌식 환경이 구축되어있는 공간에서 실습위주의 수업을 진행하여 case by case식의 경험 축적이 필요 - 특이사항발생시 실무에서 어떻게 업무를 처리하는지 등을 교육함. |
| 실무를 가르치는 강사는 현업 전문가를 초빙하여 실제 업무에서 활용 가능한 업무 스킬을 습득할 수 있는 교과 과정 설계 희망 |
| 증거자료를 확보하더라도 법적인 증거 능력을 확보 할 수 있도록 체계적이고 분석적인 보고서 작성 능력이 필요함. 수사기법 및 각종 법률적 지식을 기반으로 보고서가 작성되므로 해당 분야 지식 요구됨 |

### 4.5 단계별 디지털 포렌식 교과과정 설계

교육 과정 설계 시 실무 지향형, 디지털 포렌식 전문가 양성이라는 큰 전제하에 학습자를 중심으로 기본 IT과목을 이수한 이후에 디지털 포렌식 응용 분야로 이수하도록 설계하였으며, 대학 교과 과정 수료 후 실무에서 효율적으로 일하기 위해 실습 과목을 전 단계에 걸쳐 실시하도록 권장하였다. 법률과목도 세분화 하여 업무에 도움이 될 수 있는 실질적인 관련 분야를 교과 과정으로 선별하였다. <표 10>은 설계된 단계별 디지털 포렌식 교과 과정이다.

<표10> 단계별 디지털 포렌식 교과과정

| 목표: 실무 지향 형 디지털 포렌식 전문가 양성 | | | |
|---|---|---|---|
| 포렌식 과목 | 디지털포렌식 개론 | 이미지 방법과 저장 기술<br>수사 인터뷰 기법<br>그래픽 파일의 복구<br>안티 포렌식 기술<br>모바일 포렌식 | 암호분석 실무<br>고급디지털 포렌식<br>역공학<br>데이터베이스 포렌식<br>시스템 포렌식<br>네트워크,인터넷 포렌식 |
| 법률 과목 | 디지털포렌식 관련 윤리<br>정보통신망법<br>개인정보보호법<br>정보통신기반 보호법 | 민사 형사 소송법<br>증거 수집 법 | 형사 절차 및 범죄수사 실무 |
| 기초 선택 과목 | 정보보안 개론<br>소프트웨어 공학<br>컴퓨터, 네트워크 통신 | 데이터베이스 실무<br>컴퓨터, 네트워크 보안<br>운영체계 | 암호학 |
| 실습 과목 | 포렌식 도구 실무 실습 | 디지털포렌식 프로젝트실습 | 침해사고 대응 실습<br>법정실습 및 인턴 |
| 과목 / 등급 | Level1 기초 | Leve2 중급 | Level3 심화 |

## 5. 결론

본 논문에서는 기존 연구가 디지털 포렌직 교육 표준 모델과 중요도, 우선순위를 고려한 교육 과정 개선 사항을 도출한 것에서 더 나아가, 최근 국내외 동향을 반영하여, 현업에 종사하는 디지털 포렌식 전문가의 의견과 설문을 바탕으로 교과 과정을 설계함에 있어 기초 선택 과목, 법률 과목, 포렌식 과목, 실무 과목으로 분류하여 각 단계별로 난이도와 실무 적합도를 고려하여 세부적인 전 학년의 교과 과정을 설계 하였다. 기존 교과과정이 이론 중심적인 것을 탈피하여 졸업 후 현장에서 바로 활용할 수 있는 실무 적합도를 높이기 위해, 실제 현업에서 빈도수가 높게 사용 중

인 도구나 실습 장비를 조사하여 실습 환경과 실무를 강조하는 교과과정을 구축하는 실효성 높은 방안을 확립하였다.

디지털 포렌식 기술은 사이버 범죄의 확대로 수요가 증가할 것으로 예상되며, 법률적 의미와 정보를 다루는 과학적 지식이 두루 필요한 융합 학문적 성격을 띠고 있다. 포렌식의 교육 세부 내용도 보안적 요소를 많이 다루었던 네트워크 포렌식에서 모바일 포렌직, 멀티미디어를 다루는 미디어 포렌식, 그리고 소셜 미디어를 대상으로 하는 소셜 포렌식 그리고 클라우드 포렌식을 다루는 등 기술의 진보와 요구에 따라 세부 내용과 교과 과정이 유연하게 편성되어 현행의 흐름을 뒷받침해야 할 것이다.

이와 더불어 실무적 법률 이론, 윤리 교육, 수사 기법, 법정 실습 및 프로젝트 진행, 인턴쉽의 운영은 실무 능력 향상을 위한 필수적인 교육 과정의 일부라 할 수 있다. 이론과 실습을 겸비한 디지털 포렌식 과정 운영과 이의 저변 확대를 위해 온라인을 활용한 디지털 포렌식 교육은 증가하는 교육 수요에 부응 하는 한 수단이 될 수 있다. 온라인 교육 과정의 특성상 비용 절감뿐 아니라 공간, 시간의 제약 없이 유연성을 제공하기에 빠르게 변화 하는 포렌식 기술에 온라인 교육을 접목하는 것은 매우 시의 적절하다고 본다.

학생들에게 다양한 오픈 소스용 포렌식 도구와 상용제품을 활용한 실습실 환경과 운영은 실무 능력을 배양 하고 필요한 기술력을 확보하여 졸업 후 실무 적응력을 높일 수 있는 방안이다.

학생, 학교, 전문가 그룹, 졸업생들의 모니터링과 피드백을 통한 교육 프로그램의 평가도 필수적으로 수행되어야한다. 추후 공학 인증과 국제적 커리큘럼의 교차 인증을 위해 교과목의 표준화가 이루어져야 하며 디지털 포렌식 관련 국제 자격증의 취득은 취업 상승율과 실무 적응력을 높이며, 자격증 취득의 장려와 이를 위한 지원 프로그램의 준비도 교육의 질을 상승시킬 수 있다.

## 참 고 문 헌


[1] 정교일, 정익래, 홍도원(2007). 디지털 포렌식 기술 및 동향. **전자통신동향분석 제22권 제11호**, 97-104.

[2] 전상덕, 홍동숙, 한기준(2006). 디지털 포렌식의 기술동향과 전망. **정보화정책 제13권** 제4호, 3-19.

[3] 노명선(2012). **국제기준에 적합한 디지털 포렌식 기술교육의 표준모델 개발.** 성균관대학교 법학 전문대학원.

[4] 김종민, 최경호, 김귀남(2012). **디지털 포렌식 전문 인력 양성 교육 과정 개선에 관한 연구.** 경기대학교.

[5] West Virginia University Forensic Science Initiative(2007). Technical Working Group for Education and Training in Digital Forensics.

[6] Timothy J. McGuire, Karon N. Murff(2006). *Issues in the Development of a Digital Forensics Curriculum.* Sam Houston State University.

[7] S. Srinivasan(2013). Digital Forensics Curriculum in Security Education. Texas A and M International University.

[8] Gary C. Kessler(2007). *The Design of an Undergraduate Degree Program in Computer & Digital Forensics.* Champlain College.

[9] Manghui Tu, Kyle Cronin, Dianxiang Xu(2012). *On the Development of Digital Forensics Curriculum.* Dakota State University.

[10] Frederick B. Cohen, Thomas A. Johnson (2010). Curriculum for Digital Forensics. *IEEE Computer Society.*

[11] Paula Thomas, Iain Sutherland, Theo Tryfonas(2009). An Analysis of the Curriculum Components of Computer Forensics Undergraduate Courses in the United Kingdom, *ITALICS Volume 8 Issue 1.*

[12] Middleses University(2009). *Programme Specification and Curriculum Map for MSc Electronic Security and Digital Forensics.*

[13] 이동임, 나현미, 정향진(2012). **전문수사관 국가 자격 화에 관한 연구(사이버수사).** 한국직업능력개발원.

[14] Hai-Cheng Chu, Kuo-Hsiung Chang, Whe Dar Lin(2010). Digital Forensics Core Curriculum Design in Higher Education in Ubiquitous Computing Era. *Tamkang Journal of Science and Engineering Vol13.* No.1 pp.89-97.

**나 현 대**

1989 덕성여자대학교
영어영문학과(인문학사)
2013~현재 숭실대학교
SW특성화대학원(석사과정)
관심분야: 네트워크, 보안, 정보보호 교육과정
E-Mail: hdrha67@daum.net.

**김 창 재**

2005 숭실대학교
정보과학대학원(이학석사)
2009 숭실대학교
컴퓨터학부(이학박사)
2013~현재 숭실대학교 SW특성화대학원 교수
관심분야: SW공학, SW아키텍처, 데이터베이스, 빅 데이터 등
E-Mail: winchang@ssu.ac.kr

**이 남 용**

1983 고려대학교
경영대학원(경영정보학석사)
1993 미시시피주립대 경영정보학
(경영정보학박사)
2012~현재 숭실대학교 SW특성화대학원 교수
관심분야: SW테스트, 품질보증, MIS, 정보보호
E-Mail: nylee@ssu.ac.kr