디지털 포렌식 전문인력 양성 교육과정 개선에 관한 연구★

김종민* · 최경호** · 김귀남***

요 약

본 연구는 디지털 포렌식 전문인력 양성을 위한 교육과정을 개선하는데 그 목적이 있다. 이를 위해 디지털 포렌식 전문인력 양성을 위한 교육과정을 제시하고 그 제시된 교육과정을 포렌식 전문가를 대상으로 설문조사를 실시해 얻은 결과를 AHP 기법을 활용하여 교육과정의 요소(포렌식개론, 시스템 포렌식, 종류별 이론 및 분석, 도구사용법, 조사실무)중 가장 합리적이고 중요도가 높은 교육과정인지를 도출할 수 있었다. 이와 같은 연구를 통해 도출된 합리적이고 중요도가 높은 교육과정을 반영하여 디지털 포렌식 전문인력 양성을 위한 교육과정을 개선하고자 한다.

Research about the development of education courses for nurturing digital forensic experts

Jong Min Kim* · Kyong Ho Choi** · Kuinam J. Kim***

Abstract

This research is to improve the education courses for nurturing digital forensic exports. To do so, the education courses for nurturing digital forensic exports were proposed and surveys targeting forensic professionals are conducted. Using AHP method, the most rational and important education courses among aspects (forensic introduction, system forensic, theories and analyses by categories, tool using, and research work) were drawn from results from the above. From this research, it is to improve the education courses for nurturing digital forensic experts applying rational courses with high status.

Key words : Digital forensics, AHP, Consistency ratio, Validity, Education

접수일(2012년 10월 12일), 수정일(1차: 2012년 10월 21일), 게재확정일(2012년 10월 22일)

★ 본 연구는 지식경제부 지역혁신센터사업인 산업기술보호특화센터지원으로 수행되었음.

* 경기대학교 산업보안학과

** 경기대학교 산업기술보호특화센터

*** 경기대학교 융합보안학과

1. 서 론

인터넷 및 네트워크의 발달로 인하여 정보기술의 급속하게 발전하게 되었다. 정보화시대를 맞으면서 디지털정보의 양도 기하급수적으로 증가하였다.

미국 버클리 대학의 한 연구에 의하면 세계에서 생성되는 정보의 약 90% 이상이 디지털 형태로 만들어지고 있다고 한다[1].

이러한 디지털화 되면서 디지털 포렌식의 기술이 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. 즉, 포렌식은 수사과정에서 과학적이고 체계적인 증거확보 절차에 따라 합법적인 증거를 산출해냄으로써 범죄자 색출 및 범죄사실의 증명을 통한 실체적 진실의 발견에 크게 기여하고 있어 포렌식 분야의 전문인력의 양성이 시급하다.[2].

따라서 본 연구에서는 디지털 포렌식의 필요성과 전문인력의 교육의 문제점을 분석하여 디지털 포렌식 분야 전문인력을 양성교육과정을 개선하고자한다.

2. 관련연구

2.1 국내 디지털 포렌식 교육 및 자격증 현황

국내의 경우 민간 중심의 관련 자격증을 운영하고 있으며 최근에는 대검찰청을 중심으로 국가 디지털 포렌식 전문가 자격증 운영을 추진 중에 있다[3].

<표 1> 디지털 포렌식 전문가 교육과정 운영 기관[3]

기관	내용
대검찰청	대검찰청 수사관 및 정부기관 수사관에 대한 디지털 포렌식 교육 과정 개설운영
경찰청	경찰수사보안연구소에 사이버범죄 수사과정, 디지털 증거분석 전문가 과정 등 교육과정개설, 매년 240명 대상 교육 실시
지식경제부	2009년부터 지식정보보안아카데미에 디지털 포렌식과정 개설 운영
한국생산성본부	포렌식 교육과정으로 '사이버포렌식 조사전문가' 과정을 포함하여 5개 과정 개설 운영
대학	경기대 산업기술보호특화센터에 '실무형 디지털 포렌식 전문가 양성과정' 개설, 동국대 국제정보대학원, 영산대 사이버경찰학과, 호원대사이버수사경찰하부 운영

디지털 포렌식 관련 자격증 제도는 국내의 경우 디지털 포렌식 전문가, 사이버 포렌식 조사 전문가 자격증이 있고 해외에는 CFCE·CCE·EnCE등이 있다[3].

<표 2> 국내·외 디지털 포렌식 자격증 현황[3]

자격증	내용
디지털 포렌식 전문가	한국인터넷진흥원에서 운영하는 자격제도
사이버 포렌식 전문가	한국생산성본부, 사이버포렌식전무가협회에서 운영중인 자격제도
CFCE (Certified Forensicss Computer Examiner)	컴퓨터 포렌식 분야의 국제 수사기관 조사관들의 모임인 IACIS(International Association of Computer Inverstigative Specialists)에서 운영하는 자격제도
CCE (Cerfified Computer Examiner)	민간 포렌식 전문가 단체인 ISFCE (International Society of Forensics Computer Examiners)에서 운영하는 자격제도
EnCE (EnCase Certified Examiner)	국제적으로 많이 사용되는 EnCase라는 컴퓨터 포렌식 도구를 만든 Guidance Software라는 회사에서 발급하는 도구에 대한 자격제도

2.2 수사기관의 디지털증거 분석 전문과정

<표 3> 수사기관의 디지털포렌식 전문과정의 교과과정으로서 입교자격으로 관련분야 2년 이상의 근무자 중 사이버범죄 수사과정 이수자로 하고 있으며 총 2주 70시간에 걸쳐 운영되고 있다. 이 과정은 전체 수업시간의 90%이상 수상하지 못하거나 연수성적 60% 미만인자, 평가과목 중 한 과목이라도 40%미만일 경우, 생활평가 과실점 40점 초과자 등은 수료증을 받지 못하게 된다[4].

<표 3> 수사기관의 디지털 포렌식 전문과정[4]

분야	교 과 목	시간	비율
총계	21과목	70	100%
소양과목	4과목	8	11%
	1. 수사와 인권	2	
	2. 기본근무자세	2	
	3. 국정철학의 이해(저탄소녹색성장)	2	
	4. 종교편향 방지 교육	2	
직무과목	14과목	56	80%
	1. 디지털 증거분석 개요 및 절차	2	
	2. 하드디스크의 구조 및 파일시스템 분석	2	
	3. 고급 네트워크 증거분석	3	
	4. 윈도우 휘발성 증거 수집·분석	3	
	5. 윈도우 시스템 분석	4	
	6. 유닉스 휘발성 증거수집 분석	3	
	7. 유닉스 시스템 분석	4	
	8. 로그파일 분석	4	
	9. 데이터베이스 수사기법	3	
	10. 해킹 및 악성코드수사 사례연구	4	
	11. EnCase를 이용한 디지털증거분석 기법	8	
	12. 증거분석프로그램 실습	6	
	13. 증거능력관련 형소법 연구	3	
	14. 직무사례 세미나	7	
기타	3과목	6	9%
	1. 입교 및 수료	2	
	2. 설문 및 평가	2	
	3. 자율학습	2	

3. 제안하는 방법

본 연구에서 디지털 포렌식 전문인력 양성교육과정을 개선을 위해 교육과정을 설정하여 교육과정의 가치 평가, 선택의 문제의 고민을 해결하기 위한 AHP 방법을 이용하였다[4][5][6]. 본 연구를 위해 포렌식 전문가들의 대상으로 설문을 하였고 설문을 분석하여

평가요소들을 계층화 하였다.

3.1 설문지 작성

각 단계의 요소에 대한 중요도를 평가하는 방법은 중요도 행렬의 고유치를 이용하여 각 요소의 상대적 중요도를 구하게 된다. 상대비교 행렬은 응답자의 상대비교 값을 이용하여 응답한 것으로 두 평가요소의 상대적 합리성 정도를 17개의 값(9, 8, 7, 6, 5, 4, 3, 2, 1 ,1/2 ,1/3, 1/4, /1/5, 1/6, 1/7, 1/8, 1/9) 중 하나로 평가하게 된다.

<표 4>은 설문지의 샘플로서 평가에 대한 특성을 세분화 하여 5가지의 대분류 항목으로 구성되었다.

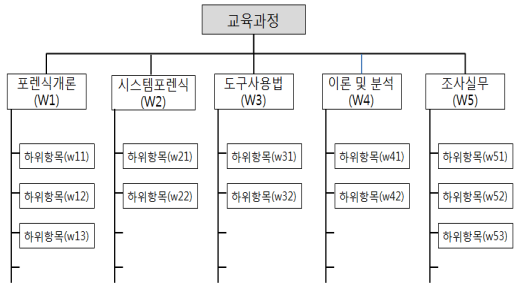
<표 4> 설문지 샘플

얼마나 더 합리적인가 평가하시오. (9, 8, … 1, 1/2, … 1/8, 1/9)	포렌식개론	시스템 포렌식	도구 사용법	종류별 이론 및 분석	조사 실무
포렌식개론	1				
시스템 포렌식	X	1			
도구사용법	X	X	1		
종류별 이론 및 분석	X	X	X	1	
조사실무	X	X	X	X	1

3.2 교육과정 계층구조

AHP 방법을 적용하여 교육과정을 개선 할 수 있다. 개발을 위해서는 교육과정의 항목 설정이 중요하다. 상대비교 행렬을 이용하여 평가요소들의 가중치를 구하고 이를 이용하여 교과과정을 산정할 수 있다.

(그림 1)은 AHP방법에 의해 교육과정의 최상위 5개 항목(포렌식개론, 시스템포렌식, 도구사용법, 이론 및 분석, 조사실무)이고, 상위 단계의 종속된 하위항목들을 보게 되면 <표 5>과 같다.



(그림 1) 교육과정 계층구조

<표 5> 하위항목 요소

구분	포렌식 개론	시스템 포렌식	도구 사용법	종류별 이론 및 분석	조사 실무
하위 항목	• 포렌식 절차 • 증거수집, 분석시 주의사항 • 민사 및 형사소송법 이론	• 리눅스, 유닉스 이론 및 실습 • 정보취득 방법 및 로그분석 방법 이론 및 실습	• SYSCheck Tool • Encase Tool	• 파일시스템, 윈도우 네트워크, 모바일 포렌식에 대한 이론 및 분석 방법	• 포렌식 프로그램 실무 • 안티포렌식 종류와 방법

4. 연구결과

본 장에서는 AHP를 이용하여 교육과정의 요소들에 대해 상대비교 행렬을 이용하여 가중치를 산출하고 산출된 값을 통해 일관성 검정을 하여 일관성 비율과 타당도를 분석하였다.

4.1 일관성 비율

AHP 방법의 장점은 상대비교 행렬을 이용하여 가중치를 산출하는 과정에서 응답자들의 일관성을 검정할 수 있다는 것이다.

상대비교 행렬을 A, 가중치 벡터를 $\underline{w}$라 하자. 행렬의 차수는 평가요소의 수는 n이다. 상대비교 행렬 A의 원소 a_{ij}는 기준요소 i의 평가요소 j에 대한

합리성의 정도 값이다.

$$A=\begin{pmatrix}1 & a_{12} & a_{13} \cdots & a_{1n}\\ 1 & 1 & a_{23} \cdots & a_{2n}\\ & & \cdots & \\ 1 & a_{n2} & a_{n3} \cdots & 1\end{pmatrix},\ \underline{w}=[w_1,w_2,\ldots,w_n]' \quad (1)$$

행렬 A에 대해 $|A-\lambda I|=\underline{0}$을 만족하는 스칼라 λ를 고유치(eigen value)라 하고, 고유치 λ에 대해 $A\underline{w}=\lambda\underline{w}$을 만족하는 벡터 $\underline{w}$를 고유벡터(eigen vector)라 한다. 상대비교 행렬 A의 최대 고유치 λ_{max}에 대응하는 고유벡터는 평가요소의 가중치를 얻는데 사용된다. 고유벡터 원소를 원소의 합으로 나누어 합이 1이 되도록 하면 그 값이 가중치가 된다.

상대비교 행렬이 완전한 일관성을 가지고 있다면 $a_{ij}a_{jk}=a_{ik}$이 성립한다. 그러나 실제 응답자가 완전한 일관성을 유지하는 것은 거의 불가능하다. 그럼 응답자의 일관성 정도를 어떻게 측정할 것인가? 완전한 일관성을 유지하지 하는 경우 $\lambda_{max}=n$이 성립하고, 그렇지 못할 경우 $\lambda_{max}>n$이 된다. 이를 이용하여 Saaty(1980)는 일관성지수(consistency index; CI)를 다음과 같이 정의하였다[7].

$$\text{일관성지수}: \quad CI=\frac{\lambda_{max}-n}{n-1} \quad (2)$$

또한, 일관성 지수를 다음 개념으로 유도하였다. 비교 요소 j에 대한 기준 요소 i의 상대적 중요도를 a_{ij}라 하고 불일치 정도를 $\delta_{ij}>-1$라 하면, 상대적 중요도는 $a_{ij}=(1+\delta_{ij})w_i/w_j$으로 표현할 수 있다. 그러면 다음 式이 성립한다.

$$\lambda_{max}-n=\frac{1}{n}\sum_{1\le i<j\le n}\frac{\delta_{ij}^2}{1+\delta_{ij}}\ge 0 \quad (3)$$

위의 式에서 평가자가 완전한 일관성을 가지면, 즉 δ_{ij}(불일치 정도)가 0이 되면 $\lambda_{max}=n$가 성립하게 된다. 이를 이용하여 일관성 지수 개념을 유도하였다.

일관성이 클수록 λ_{max} 가 n에 가까워진다. 따라서 다음과 같은 CR(일관성 비율)을 사용하여 일관성의 정도를 측정할 수 있다.

$$CR(\text{일관성 비율})=\frac{CI(\text{일관성 지수})}{RI(\text{난수 지수})} \quad (4)$$

여기서 CI는 일관성지수로써 일관성이 클수록 0에 가까운 값을 가진다. RI는 Ramdom Index로 1~9사이의 난수를 사용해서 구성한 비교행렬의 CI들의 평균값이다.

<표 6> 설문 응답자의 일관성비율

응답자	최대 고유치 λ_{max}	일관성 지수 CI	일관성 비율 CR (%)
1	11.092	1.523	1.360
2	8.685	0.9210.	0.823
3	10.877	1.469	1.312
4	14.158	2.290	2.044
5	12.984	1.996	1.782
6	9.823	1.206	1.077
7	13.161	2.040	1.822
8	13.985	2.246	2.006
9	10.132	1.283	1.145
10	11.104	1.526	1.363

<표 6>은 교육과정 요소(포렌식개론, 시스템 포렌식, 종류별 이론 및 분석, 도구사용법, 조사실무)에 대한 상대 합리성을 평가한 응답자 10명의 상대비교 행렬로부터 얻어진 최대 고유치와 일관성지수, 일관성 비율(난수 지수=1.12)을 정리한 것이다. 모든 응답자가 일관성 비율이 0.1 미만으로 나와 모두가 평가에 대한 일관성을 나타냈다.

4.2 타당도 분석 결과

<표 7> 평가요소 타당도 분석 결과

	포렌식 개론	시스템 포렌식	도구 사용법	종류별 이론 및 분석	조사 실무	결과
포렌식 개론	1	1.851	0.419	1.530	0.363	0.160
시스템포렌식	0.540	1	0.283	0.786	1.393	0.132
도구사용법	2.386	3.533	1	1.308	1.561	0.334
종류별 이론 및 분석	0.653	1.272	0.764	1	0.662	0.159
조사 실무	2.754	0.717	0.640	1.510	1	0.215
C.I (일관성 지수) = 0.651 C.R (일관성 비율) = 0.581						

<표 7>의 최대 고유치 λ_{max}는 7.602이다. 이것을 式(2)에 대입하여 일관성 지수를 알아보면 0.651이고 式(4)에 대입하여 일관성 비율을 보면 0.581%(10%미만)로 그룹 전체가 평가의 일관성을 유지하고 있음을 알 수 있다.

<표 7>의 1행 2열의 1.851은 다음 계산 절차에 의해 계산되었다.

- 응답자 1의 1행 2열 원소 값=3
- 응답자 2의 1행 2열 원소 값=2
- 응답자 3의 1행 2열 원소 값=3
- 응답자 4의 1행 2열 원소 값=3
- 응답자 5의 1행 2열 원소 값=1
- 응답자 6의 1행 2열 원소 값=1
- 응답자 7의 1행 2열 원소 값=7
- 응답자 8의 1행 2열 원소 값=1
- 응답자 9의 1행 2열 원소 값=0.25
- 응답자 10의 1행 2열 원소 값=5

그러므로 4개 값의 기하 평균은

$$\sqrt[10]{3\times2\times3\times3\times1\times1\times7\times1\times0.25\times5}=1.851$$

이다. 그리고 5개의 평가요소 중 도구사용법의 항목이 가장 높게(0.034) 나타나 디지털 포렌식 전문인력 양성에 대한 교재개발 항목 중 가장 합리적으로 나타났다. 그 뒤로 조사실무(0.215), 포렌식개론(0.160), 종류별 이론 및 분석(0.159), 시스템 포렌식(0.132)의 순서로 나타나고 있다.

5. 결 론

인터넷 및 네트워크의 발달로 인하여 정보기술의 급속하게 발전하게 되었다. 정보화시대를 맞으면서 디지털정보의 양도 기하급수적으로 증가하였다.

이러한 사회 모든 분야가 디지털화 되면서 디지털화된 증거를 수집하고 분석을 하기 위한 포렌식 전문인력의 양성이 무엇보다도 시급하다.

이 연구에서는 디지털 포렌식 전문인력 양성교육과정 개선을 위해 교과과정을 제시하고 제시된 교육과정을 포렌식 전문가의 설문으로 통해 교과과정의 상대적 중요도와 우선순위를 제시하여 교육과정을 제안하고자 하였다.

<표 8> 포렌식 교육과정 편성

순위	구분	교육과정	세부 과목명
1	실습	도구사용법	• SYSCheck Tool • Encase Tool
2	이론 및 실습	조사실무	• 안티포렌식 종류와 방법 • 포렌식 프로그램 실무
3	이론	디지털 포렌식개론	• 디지털 포렌식의 이론, 민사 및 형사소송법 이론
4	이론 및 실습	포렌식 종류별 이론 및 분석	• 종류별 이론 및 분석 방법
5	이론 및 실습	시스템 포렌식	• 리눅스, 유닉스 이론 및 실습

<표 8>은 우선순위를 두어 교육과정을 제안하여 편성한 결과로 디지털 포렌식 전문인력 양성교육에 가장 합리적인 교과과정은 포렌식 도구사용법의 과정으로 SYSCheck Tool과 Encase Tool에 대한 사용법의 실습을 학습하여 이로 인한 실무적인 교육이 가장 합리적이고 우선시 되는 교과과정으로 나타났다. 그 뒤로 안테포렌식의 종류와 방법에 대해 학습하는 포렌식 조사실무, 디지털 포렌식의 이론 및 민사 및 형사소송법에 대해 학습을 하는 디지털포렌식개론, 포렌식 종류별 포렌식 이론 및 분석, 리눅스, 유닉스의 정보취득 방법과 로그 분석 방법 학습을 하는 시스템 포렌식의 순으로 연구결과를 얻을 수 있었다.

이 연구의 결과를 토대로 디지털 포렌식 전문인력 양성 교육과정이 보다 실무에서 활용할 수 있는 교육과 교육을 통한 디지털포렌식관련 서비스를 제공하는 기관등의 현장에 바로 투입될 수 있는 교육과정을 중점적으로 반영하여 진행하여야 할 것이다.

참고문헌

[1] 탁희성, 이상진, “디지털 증거분석도구에 의한 증거수집절차 및 증거능력 확보방안”, 한국형사정책연구원, 2006.

[2] 곽병선, “디지털 포렌식 수사의 문제점과 개선방안”, 한국법학회지 제42집, p. 173, 2011.

[3] 방송통신위원회, 국가정보보호백서 pp. 310-312, 2011.

[4] 이정표, “디지털포렌식 수사관 자격제도 운영방안”, 대검찰청, 2009

[5] Aczel, J.and Saaty, T.L., Procedures fro synthesizing ratio judgement, Journal of Mathematical Psychology, 27, pp.99-102, 1983.

[6] Goldberger, A.S. Structural Equations Methods in the Social Science, Econometrica, 40, 979-1001, 1980.

[7] Ramanathan,R.and Ganesh,L.S.,Group preference aggregation methods employed in AHP: An evaluation and an intrinsic process for deriving members' weights, European Journal of Operational Research, 79.pp.249-264, 1994.

[8] Saaty, T.L., Wong,M.M The Analytic Hierarchical Process, New York; McGraw Hill, 1980

[저자소개]

김 종 민(Jong-Min Kim)

2012년 현재 경기대학교 산업보안학과 박사과정

email : dyuo1004@gmail.com

최 경 호(Kyong-Ho Choi)

2002년 경기대학교 경제학사
2005년 경기대학교 경제학석사
2008년 경기대학교 정보보호학박사
2012년 경기대학교 연구교수
(산업기술보호특화센터)

email : cyberckh@gmail.com

김 귀 남(Kuinam J. Kim)

Univ. of Kansas 수학과 학사
Colorado State Univ. 통계학 석사
Colorado State Univ. 산업공학 박사

현재 경기대학교 융합보안학과 교수
산업기술보호특화센터장

email : harap123@hanmail.net