Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.4, Aug. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.4.647

경찰 디지털증거분석관 역량모델 개발*

오 소 정,[1†] 정 준 선,[2] 조 은 별,[2] 김 기 범[3‡]
[1,3]성균관대학교 (대학원생, 교수), [2]경찰대학 (교수)

Development of Competency Model for Police' Digital Forensic Examiner*

Oh SoJung,[1†] Jeong JunSeon,[2] Cho EunByul,[2] Kim GiBum[3‡]
[1,3]Sungkyunkwan University (Graduate student, Professor),
[2]Korean National Police University (Professor)

요 약

범죄수사에서 디지털증거가 중요해지면서 법정에서 다툼이 많아지고 있다. 매체가 다양화되고 분석범위가 확장되면서 디지털포렌식에 대한 전문성 수준도 높아지고 있다. 그러나 아직까지 디지털증거분석관의 역량을 정의하거나 전문성을 판단하는 역량모델 개발은 이루어지지 않고 있다. 디지털증거분석관에게 필요한 역량을 도출한 일부 연구가 있었으나 여전히 미흡한 수준이다. 따라서 본 연구에서는 전문가 FGI, 델파이 조사 등의 방법론을 활용해 총 9개의 역량군 25개의 역량평가 요소를 정의하였다. 구체적으로 디지털포렌식 이론, 디지털증거 수집 및 관리, 디스크포렌식, 모바일포렌식, 영상포렌식, 침해사고포렌식, DB포렌식, 임베디드(IoT)포렌식, 클라우드포렌식으로 규정하였다. 디지털증거분석관 역량모델은 향후 선발, 교육훈련, 성과평가 등 다양한 분야에 활용할 수 있을 것으로 기대한다.

ABSTRACT

As digital evidence becomes more important in criminal investigations, disputes are increasing in court. As media diversifies and the scope of analysis expands, the level of expertise in digital forensics is also increasing. However, no competency model has been developed to define the capabilities of digital evidence examiners or to judge their expertise. There have been some studies that have derived the capabilities necessary for digital evidence examiner, but they are still insufficient. Therefore, in this study, 25 competency evaluation factors in a total of 9 competency groups were defined using methodologies such as expert FGI and Delphi survey. Specifically, it was defined as Digital Forensics Theory, Digital Evidence Collection&Management, Disk Forensics, Mobile Forensics, Video Forensics, infringement forensics, DB Forensics, Embedded(IoT) Forensics, and Cloud Forensics. The digital evidence examiner competency model is expected to be used in various fields such as recruitment, education and training, and performance evaluation in the future.

Keywords: Digital Forensic Examiner, Competency Model, Competency Evaluation, Digital Forensics, Digital Evidence

I. 서 론

디지털포렌식이 범죄수사에서 필수적인 수사기법으로 자리 잡았다[1]. 과거에는 법정에서 물리적 증거가 대부분을 차지하였으나 최근에는 디지털증거가 대세를 이루고 있다[2]. 디지털증거는 성착취물을 제작하고 유포한 사건, 산업기술을 유출한 사건 등 사회적으로 문제가 되는 사건에서 핵심적인 증거가 되고 있다[3].

디지털증거분석관(이하, 분석관)은 일정한 자격과 전문지식을 갖춰 디지털증거 분석 의뢰를 받아 수행하는 역할을 한다. 분석관은 디지털증거 처리에 대한

Received(06. 02. 2023), Modified(06. 27. 2023), Accepted(06. 27. 2023)
* 이 연구는 2022년 경찰청 디지털 증거분석관 맞춤형 교육과정 설계 및 운영 사업에서 수행한 연구내용을 수정·보완한 것임
† 주저자, mira0809@naver.com
‡ 교신저자, freekgb02@gmail.com(Corresponding author)

기술과 법률뿐만 아니라 절차에 대한 전문성까지 보유해야 한다[4]. 한국인정기구(Korea Laboratory Accreditation Scheme; KOLAS)는 분석관에 대해 공인 숙련도 시험기관(ISO/IEC 17043), 공인 시험기관(ISO/IEC 17025) 인정을 통해 신뢰성을 부여하고 있다[5]. 그러나 최근, 법정에서 디지털 증거에 대한 증거능력을 판단하는 기준이 엄격해지면서 분석관의 전문성이 쟁점이 되고 있다[4]. 더구나 범죄환경이 메타버스, 클라우드 등으로 다양해지면서 분석관에게 요구하는 역량의 수준도 높아지고 있다[6]. 분석관은 새로운 기술에 대비하여 디지털포렌식 분야를 파악하고 부족한 역량을 찾아내 교육훈련을 받아야 한다[1]. 소속기관에서는 기존 교육과정 분석을 통해 역량을 도출하고 우선순위를 정해 운영할 필요가 있다[7]. 그간, 디지털포렌식과 관련하여 전문가 역량 우선순위[8], 전문가 자격제도[9], 전문인력 양성 교육과정[10], 전문인력 양성 평가지표[11] 등에 대한 연구가 이루어졌을 뿐 역량에 대한 체계적인 연구는 미흡한 수준이다.

따라서 본 연구에서는 경찰 분석관이 디지털포렌식을 수행하는데 필요한 역량을 도출하여 역량모델을 개발하고자 한다. 제2장에서 분석관의 직무를 상세 분류해 요소를 도출하고 역량과 역량모델에 대한 정의를 살펴본다. 제3장에서는 역량요소 도출과 타당성 검증을 수행하고 제4장에서는 잠정 역량모델을 검증하여 최종적인 역량모델을 확정한다.

II. 디지털증거분석관의 직무와 역량

2.1 디지털증거분석관의 개념과 자격

분석관은 '디지털포렌식을 수행하는 사람으로서 디지털증거를 처리할 수 있도록 관련 교육이나 실무를 수행하고 일정한 역량을 갖춘 사람'으로 정의할 수 있다. 경찰청 '디지털증거의 처리 등에 관한 규칙'(이하 '규칙'이라 한다)에서 분석관은 '전자정보를 수집, 보존, 운반, 분석, 현출, 관리 시 필요한 지식이나 전문기술을 보유한 사람 중에서 선발되어 디지털증거분석 의뢰를 받고 이를 수행하는 사람'을 말한다.(제2조, 제6조) 디지털포렌식은 "전자정보를 수집·보존·운반·분석·현출·관리하여 범죄사실 규명을 위한 증거로 활용할 수 있도록 하는 과학적인 절차와 기술"(제2조 제2호)라고 정의하고 있다.

경찰청의 분석관 선발요건은 ① 관련 전문교육을 수료하거나 ② 관련 분야에서 3년이상 근무 혹은 공학·전자공학·정보보호학 등 관련 분야 석사 이상의 학위를 소지했거나 ③ 관련 분야 학사학위를 소지한 자 중, 전문교육 과정을 수료했거나 자격증을 소지할 것을 요구한다(제6조). 3년 이상의 근무경력이나 학위, 자격증 등으로 세분화하며 객관적인 전문성을 요구하는 반면, 대검찰청 예규 '디지털증거의 수집·분석 및 관리 규정'(이하, '대검찰청 예규')에서는 디지털포렌식 수사관의 자격요건으로 전문가 양성과정을 이수 또는 국내외 컴퓨터 관련 교육과정을 이수한 자로서 디지털포렌식 관련 지식이 충분한 자라고 규정하고 있다.(제9조) 대검찰청은 관련 지식의 충분성과 같은 주관적인 기준을 규정하고 있다. 또한 분석관이 압수수색과 같은 수사실무도 담당하는 것과 달리(대검찰청 예규 제11조 제1항, 제14조) 경찰청은 디지털증거 처리과정 전반을 전담한다.

2.2 디지털증거분석관의 직무

디지털포렌식 결과가 법정에서 유죄를 입증하는 단서로 사용되면서 분석관의 전문성이 쟁점이 되고 있다. 법원은 디지털증거의 증거능력 인정에 있어 '컴퓨터의 기계적 정확성, 프로그램의 신뢰성, 입력·처리·출력 각 단계에서 조작자의 전문적인 기술능력과 정확성'까지 요구하고 있다.(대법원 2013도2511)

분석관은 디지털포렌식 즉, 디지털증거의 분석을 직무로 한다.(규칙 제2조 제8호) 분석관 업무를 순서대로 살펴보면 먼저, 경찰관의 요청에 의해 디지털증거 수집에 대한 기술적인 지원을 한다.(규칙 제10조) 수사현장에서 정보저장매체의 복제본 또는 원본을 반출하여 현장 이외의 장소에서 압수·수색·검증을 수행한다.(규칙 제18조) 경찰관이 분석관에게 증거분석을 의뢰하고자 할 경우, 의뢰 전까지 경찰관이 동일성, 무결성, 연계보관성 등에 대한 책임을 지지만(규칙 제23조) 의뢰된 후에는 분석관에게 이전된다.(규칙 제24조) 나아가, 분석관은 의뢰물에 대한 분석과 결과보고서를 작성하고(규칙 제3장, 제4장) 경찰관에게 회신될 때까지 관리 책임을 진다.(규칙 제34조, 제35조, 제36조) 분석관의 직무는 전문적인 컴퓨터 기술에 관한 것을 주(主)로 하되 디지털증거에 대한 법제와 절차를 포함한다[12]. 각 단계별 정도의 차이는 있으나 디지털증거 처리 전반에 걸쳐있다. 따라서 분석관에게 필요한 역량요소를 도출하고자 할 때는 양자를 모두 고려해야 한다.

2.3 디지털증거분석관의 역량

역량이란 개인이 특정 업무를 수행하는 데 있어 높은 수준의 직무성과를 도출할 수 있게 만드는 내재적인 특성을 말한다[13]. 관찰과 측정이 가능한 기준으로 표현되어야 하고 정확한 기준으로 진단할 수 있어야 한다[14]. 1920년대 Frederick Taylor가 일을 가장 효과적으로 할 수 있도록 다양한 요소로 나누고 이를 '관리능력(Management Competency)'으로 정의하면서 사용되기 시작하였다[15]. 이후, 다양한 학자들에 의해 개념화되었고 '성과와 직결되는 요소'임을 강조하고 있다[17]. 기존에는 객관적으로 습득되는 지식, 업무의 절차를 다루는 기술, 개인적 특성 및 기질로 구분하였으나[16] 현재는 지식, 기술, 태도 또는 능력으로 구분해 사용하고 있다[17]. 역량모델은 "조직 목적 달성에 결정적인 영향을 미치는 핵심적인 사항인 역량을 규정하고 성공적이고 안정적인 성과 창출을 위해 필요한 기준과 방향을 체계적으로 결정하는 과정" 즉, 역량모델링(Competency Modeling)의 결과를 말한다[14].

분석관은 디지털증거를 수집하여 분석할 수 있는 과학적 지식과 기술뿐만 아니라, 다양한 위기 상황에 적절하게 대응할 수 있어야 한다[1]. 분석기술에 대한 전문성뿐만 아니라 증거능력을 위해서 '조작자의 전문성' 입증도 중요하다. 예컨대, 미국은 연방증거법 제702조에서 전문가의 요건으로 '지식, 기술, 경험, 훈련 또는 교육'을 명시하고 있다. 또한 고도의 기술은 필요하지 않고 일반적인 수준의 전문성을 요구하고 있다. 즉, 미국은 전문성 판단에 있어 컴퓨터 프로그래밍, 프로그램 코드 해석 등의 배경지식을 요구하지 않고 분석을 해본 경험이 있거나 일정한 교육훈련을 이수하고 오류를 증언할 수 있다면 충분하다는 입장이다[29, 30].

그간, 분석관의 역량요소를 도출하고자 하는 시도는 종종 있었으나 분석관의 직무를 명확히 하면서 역량요소를 도출한 경우는 확인할 수 없었다. 대표적으로 이윤정등은 디지털포렌식 전문인력을 기초, 고급 수준으로 구분하고 네트워크 보안, 윤리 등 새로운 기술적 역량을 발굴하였으나 분석관이 갖춰야 하는 전반적인 역량은 도출하지 않았다[10]. 신준우도 디지털포렌식 전문인력을 양성하기 위한 대학 교육과정을 제시하면서 전문가에게 요구되는 역량(기술)들을 분석하였으나 분석관에게 방점이 있다고 보기 어렵다[18]. 김기범등은 디지털포렌식 전문가 자격 부여를 위한 조건으로 지식·기술·태도를 구분하여 직무분석을 하였지만 현재 기술환경에 비추어볼 때, 적용하는데 한계가 있다[9]. 박희일등은 디지털포렌식의 수준을 평가하기 위해 조직·인원·기술·시설·절차 등 평가지표를 개발하고 직·간접적으로 분석관의 역량요소를 제시하였지만 선행연구 내지 국내외 평가지표를 분석하는 수준에 그쳤다[11].

교육과정, 조직을 재설계하거나 전문성 향상을 목표로 설문을 통해 개선하려는 시도도 있었다. 김현주등은 디지털포렌식 역량강화를 위해 교육과정 재설계가 필요하다고 하였으나 개별적인 역량요소를 도출하지 않고 설문은 분석관이 아닌 현장경찰관을 대상으로 하였다[1]. 나현대등도 대학 교과과정을 설계하고자 분석관을 대상으로 설문을 하였으나, 교과과정의 적합도 검증에 그쳤다[19]. 신지호등은 디지털포렌식 조직구조, 업무과정 개선을 목표로 인터뷰를 하였고[13] 김남명등은 경찰 디지털포렌식의 신뢰성과 전문성 향상방안을 목적으로 수행하였다[12]. 한편, 역량요소를 도출한 경우도 있었다. 윤혜정등은 AHP(Analytic Hierarchy Process, 계층적 분석방법)를 적용해 디지털포렌식 전문가에게 필요한 역량 항목 20개 중에서 장비 및 도구 활용, 저장매체 데이터 추출 및 이미징 기술, 파일시스템 및 운영체제 관련 지식, 디지털증거 관련 법률에 대한 이해 등 중요도가 높다고 하였다[8]. 그러나 역량요소 도출은 주로 선행연구를 활용해 현재 요구도 수준에 부합하지 않고 이미 도출된 상태에서 검증을 위해 비로소 분석관의 인터뷰, 설문을 활용하였다.

III. 디지털증거분석관 역량모델 연구방법

3.1 디지털포렌식 역량요소 도출절차

역량요소 도출은 문헌연구, 전문가 FGI(Focus Group Interview), 델파이 조사 등의 방법론을 활용하였다.〈표 1〉 먼저, 선행연구에 기반한 분석관의 역량모델을 도출하였다. 타당도 검증과 보완을 위해 현장전문가 대상으로 델파이 조사(Delphi Method)를 실시하였다. 델파이 조사는 쟁점 분야의 전문가를 대상으로 의견을 반복적으로 수집·교환·수정하는 과정을 거쳐 합의된 의견을 이끌어내는 주·직관적인 방법이다[11]. 양적으로 측정이 곤란할 때 다양한 전문가 의견을 종합해 변화하는 사회과학적 쟁점을 하나로 수렴하는데 적합하다[20].

Table 1. Procedure for deriving competency elements of digital evidence analyzer

DIV	Procedure	Contents
Step 1	Literature Review & Field Experts Focus Group Interview	· Preliminary review for analysis of prior studies and derivation of competency model · In-depth interviews with expert digital forensic examiners in the field · Derivation of tentative competency model including competency group, name, definition, etc
Step 2	Delphi Survey	· Validation of competency model · Revision and enhancement of competency group, name, definition
Step 3	Finalization of Competency Model	· Analysis and review of Delphi survey results and expert opinion on descriptive responses Finalization of competency group · names, and definitions based on field experts' feedback

다만, 조사대상에 따라 연구의 결과가 달라질 수 있다는 한계가 있다[21]. 이를 해소하기 위해 경찰청 소속 전문가 3명의 자문을 거쳐 1차, 2차 델파이 조사 질문지를 확정하고 최종적으로 분석관의 역량군과 역량요소를 도출하였다.

1단계에서 선행연구를 통해 역량군, 역량요소 등을 정의하고, 이에 대해 2022년 7월 6일부터 7월 11일까지 총 3회에 걸쳐 전문가 FGI(Focus Group Interview)를 실시해 잠정 역량모델을 도출하였다. 전문가는 경찰청에서 디지털증거분석 업무에 우수한 성과와 능력을 보유하고 있다고 추천한 경찰관 3명과 경찰수사연수원 교수 1인을 포함해 총 4인을 선정하였다.

2단계에서는 잠정 역량모델을 기반으로 전문가 집단에게 2회에 걸쳐 델파이 조사를 수행[16]하는 '수정된 델파이 조사(Modified Delphi technique)'[23]를 실시하였다. 결과 분석을 통해 각 역량에 대해 개선, 수정하였다. 온라인 서면조사를 통해 1회차는 6일간(2022년 7월 14일~7월 20일), 2회차는 8일간(2022년 8월 31일~9월 7일) 진행하였다. 전문가그룹은 학계, 산업계, 실무 등 3개 그룹으로 세분화하여 디지털증거분석의 모든 영역을 포괄할 수 있는 기준을 설정해 선정하였다.〈표 2〉

Table 2. Criteria for expert panel selection n delphi survey

Div	Selection Criteria
Academia	Individuals with a doctoral degree or higher, possessing over 10 years of research experience in the relevant field, and demonstrating a comprehensive understanding of law and technology
Industry	Individuals engaged in industries such as corporate enterprises and research institutes, possessing a sufficient understanding of the relevant industry, and having experience participating in tool development and lab establishment projects
Field Expert	Individuals currently employed in the police force and actively engaged in operational duties, possessing a comprehensive understanding of the police landscape and practices, and having received internal training in the field of digital forensics

1회차에서는 각 분야 5명씩 총 15명 대상 잠정 역량모델에 대한 내용타당도(Content Validity Ratio, CVR)를 검증하였다. CVR은 측정하고자 하는 구성개념을 얼마나 적절히 반영하고 있는가에 대한 것이다[23].

$$CVR = \frac{n_e - (N/2)}{N/2} \quad (1)$$

※ N: 응답자 수, n_e: 필수적이라고 응답한 수

2회차에서는 1회차에서 회신된 결과를 수정·보완한 내용에 대해 내용타당도를 검증하였다. 전문가는 각 분야에 경험을 보유한 3명을 추가하여 총 18명을 대상으로 실시하였다.〈표 3〉

3단계에서는 델파이 조사결과로 수집한 자료를 분석해 최종 역량모델에 반영하였다. 선행단계에서 도출된 내용타당도, 긍정응답률, 표준편차, 수렴도, 합의도, 안정도 결과를 검토해 적합하다고 판단된 항목을 선별하였다. 서술형으로 제시된 응답은 전문가 의견을 종합하고 연구진의 합의를 거쳐 항목별로 채택 여부를 확정하였다.

Table 3. Expert Panel Selected for Delphi

No	Domain	Education	Activity Period(Month)
1	Academia	Ph.D.	136
2	〃	〃	204
3	〃	〃	300
4	〃	Ph.D. Complete	128
5	〃	Ph.D.	156
6	Industry	Ph.D. Complete	142
7	〃	〃	162
8	〃	Ph.D.	126
9	〃	Master Complete	193
10	〃	Ph.D. Complete	168
11	Police	Master	143
12	〃	〃	156
13	〃	〃	137
14	〃	〃	194
15	〃	〃	184
16	All	〃	218
17	〃	〃	200
18	〃	〃	140

3.2 역량평가 모델 타당성 검증 방법

역량평가 모델의 타당성은 3가지 순서로 검증하였다. 먼저, 선행연구와 국가직무능력표준(NCS)에 정의된 관련 역량을 반영하여 역량모델 초안을 작성하였다. 다음으로는 FGI 과정에서 분석관에게 적합하고 수용 가능한 역량명과 역량정의를 작성하도록 하였다. 마지막으로 연구진의 숙의를 거쳐 세부 내용을 수정, 삭제, 보완하여 잠정 역량모델을 도출하였다.

역량모델의 타당성을 검증하기 위해 델파이 조사 결과를 분석하여 전문가그룹의 일치된 의견을 채택하였다[16]. 구체적으로 1차 델파이 결과는 CVR를 중심으로, 2차 델파이 결과는 CVR, 긍정응답률 및 표준편차, 수렴도, 합의도, 안정도를 산출하여 분석하였다. 역량 채택 여부에 대해 1차 델파이에서는 예/아니오로 응답하게 하여 산출하였고 2차 델파이에서는 5점 Likert 척도로 응답한 결과를 바탕으로 1~3점은 '아니오', 4·5점은 '예'로 치환하여 분석하였다. 전문가 집단은 1차 15명, 2차 18명으로 CVR .49 이상을 최소값으로 설정하였다. 이때, 전문가 합의 여부를 판단하기 위한 CVR 기준은 Ayre와 Scally의 방법론을 채택하였다. Lawshe가 제안한 CVR은 델파이 조사에 참여한 전문가의 수에 따라 결정된 최소값 이상이 되었을 때 해당 문항이 타당하다고 판단하는 방법이다[24]. Ayre와 Scally는 Lawshe에 의해 제안된 CVR 산출 방식의 문제점을 개선하여 이항 확률 계산에 기초한 수정된 CVR 최소값을 제안하였다[24]. Ayre와 Scally의 기준에 의하면, 본 연구에 참여한 전문가 수가 15명일 때 CVR 값은 .600 이상, 18명일 때 CVR 값은 .444 이상이어야 한다.

전문가 의견 수렴도(Convergence)는 사분위수 범위(IQR)를 2로 나눈 값으로 5점 척도에서 50% 이상의 전문가가 같은 점수를 주었다면 수렴도는 0이 된다[25]. 50% 이상의 전문가가 비슷한 점수를 주었는지를 측정한다. 따라서 본 연구에서 수렴도는 0 이상의 양수 값을 가지며 .5 이하이면 일정하게 결과값이 수렴하였다고 판단할 수 있다[26]. 합의도(Consensus)는 50%의 전문가가 어느 구간에서 비슷한 점수를 주었는지를 의미한다. 1에서 사분위수 범위를 중앙값으로 나눈 값을 빼는 방식으로 결정한다. 합의도의 최대값은 1이며 델파이에서는 .75 이상이면 합의가 이루어졌다고 판단한다[24]. 안정도(stability)는 반복되는 조사에서 응답의 일치성이 높다고 할 수 있는지를 나타낸다[27]. 산술평균으로 표준편차를 나눈 값인 변이계수(Coefficient of Variation)를 사용하며 .5 이하인 경우에는 안정된 것으로 .5 ~ .8 구간인 경우에는 비교적 안정적인 것으로 .8 이상이면 합의가 이루어지지 않은 것으로 판단할 수 있다.

$$\text{수렴도(Convergence)} = \frac{Q_3 - Q_1}{2} \tag{2}$$

$$\text{합의도(Consensus)} = 1 - \frac{Q_3 - Q_1}{Mdn} \tag{3}$$

$$\text{안정도(cv)} = \frac{SD(\text{표준편차})}{\overline{X}(\text{평균})} \tag{4}$$

CVR의 결과값에 따른 판단기준은 Lawshe과 Ayre&Scally의 기준을 혼용하여 .600 이상이면 채택, .600 ~ .490 구간이면 재검토, .490 미만이면 기각으로 분석기준을 설정하였다. 또한 전문가 의견의 일치도를 확인하기 위해 선행연구를 참조하여 평

균은 4.0 이상, 표준편차는 .8 미만, 수렴도는 .5 미만, 안정도는 .8 미만, 합의도는 .5 이상에 해당하는 항목을 확정하는 것을 분석기준으로 설정하였다[26]. 델파이 분석결과가 분석기준에 해당하지 않더라도 해당 항목을 포함시켜야 할 타당한 근거가 있는 경우에는 연구진 합의를 통해 채택하되, 구체적인 사유를 서술하였다.

IV. 디지털증거분석관 역량모델 연구결과

4.1 디지털증거분석관 잠정 역량 모델

FGI 결과를 종합해 9개 역량군, 25개 역량으로 구성된 잠정 역량모델을 도출하였다. 각 역량모델에 해당하는 역량정의와 행동지표도 함께 구성하였다. 먼저, 역량군은 디지털포렌식 이론, 디지털증거 수집 및 관리, 디스크포렌식, 모바일포렌식, 영상포렌식, 침해사고포렌식, DB포렌식, 임베디드(IoT)포렌식, 클라우드포렌식 등 9개로 구성하였다.

Table 4. Tentative Competency Model for Examiner

Cluster	Competency Factor	
Digital Forensic Theory	· Securing Integrity · Creation of Replication · File System	· Timeline Analysis · File Analysis · Encryption and Decryption
Digital Evidence Collection & Management	· On-site Digital Evidence Collection · Forensic Lab Management · Evidentiary Testimony	
Disk Forensics	· Acquisition of Disk Data · Analysis of Disk Data	
Mobile Forensics	· Acquisition of Mobile Data · Analysis of Mobile Data	
Video Forensics	· Analysis of Video Data	
Incident Response Forensics	· Acquisition of Network Data · Analysis of Network Data · Malicious Code Acquisition · Malicious Code Analysis	
DB Forensics	· Acquisition of DB Data · Analysis of DB Data	
Embedded Forensics	· Embedded(IoT) Basics · Acqusition of Embedded(IoT) Data · Analysis Embedded(IoT) Data	
Cloud Forensics	· Acquisition of Cloud Data · Analysis of Cloud Data	

'디지털포렌식 이론'(Digital Forensics Theory) 역량군은 분석관이 수행하는 업무에 있어 기본적인 지식을 알고 디지털증거를 수집, 분석하는 역량이다. 즉, 디지털증거를 수집, 분석, 보고하여 법적 효력을 갖도록 하는 기술에 관한 것이다[28]. 디지털포렌식에서 장비/도구 프로그램 활용과 데이터 추출, 이미징 기술은 증거분석을 위한 기초적인 역량이라고 할 수 있다. 파일시스템 구조, 암복호화 등 전문지식을 기반하거나 타임라인 분석을 통해 사건을 재구성하거나 분석 대상을 파악하는데 필요하다. 즉, 컴퓨터공학과 관련된 전문성을 활용하고 증거를 추출할 수 있는 기술적 역량에 대한 수준을 평가한다.

'디지털증거 수집 및 관리'(Digital Evidence Collection&Management) 역량군은 디지털증거 수집, 분석, 관리 등의 업무에 있어 지침이나 규정 등 인지하고 준수하는 역량이다. 분석관은 디지털증거를 법정에 제출하여 증거능력을 다투어야 하기 때문에 법제와 절차에 대한 이해가 필요하다[4]. 분석관은 디지털증거를 다루는 자신의 행위 모든 범주에서 절차를 준수해야 한다. 증거능력은 현장에서 증거수집 방법, 증거 보관 방식과도 관련이 있다. 즉, 디지털증거의 무결성을 훼손하지 않도록 적법한 절차를 준수하여 수집·분석·관리하고, 법정에서 증언할 수 있는지 평가한다.

'디스크포렌식'(Disk Forensics) 역량군은 디스크에 저장된 데이터를 수집하고 혐의를 입증하는 데 필요한 정보를 복구, 분석하는 역량이다. 분석관은 매체의 상태를 점검해 적합한 방식으로 이미지를 획득하고, 휘발성데이터 수집에 대한 판단, 도구·장비 활용, 훼손된 증거에 대한 원상복구를 수행하는 분석기술이 필요하다. 또한 수집된 방대한 자료에 대해 라벨링, 정규표현식 등을 통해 사건과 관련된 증거를 구별할 수 있어야 한다. 즉, 다양한 아티팩트를 추출하고 해석할 수 있는지를 평가한다.

'모바일포렌식'(Mobile Forensics) 역량군은 모바일 등 휴대용 기기에 저장된 데이터를 수집하고 혐의를 입증하는 데 필요한 정보를 복구, 분석할 수 있는 역량이다. 모바일 매체 분석 도구는 비교적 정형화되어 있으나 새로운 버전의 운영체제가 출시되면 다른 분석기술이 요구될 수 있다. 또한 도구·장비를 통해 기기에서 수집할 수 있는 정보가 한정되어 있기 때문에 어플리케이션의 로그 등을 추출해 분석해야 한다. 즉, 도구 조작능력과 어플리케이션에서 사용자의 행위 데이터를 해석할 수 있는지를 평가한다.

'영상포렌식'(Video Forensics) 역량군은 CCTV, 블랙박스 등 영상기기에 저장된 영상을 변환하거

나 복원, 촬영일시 확인 등을 통해 혐의를 입증하는 역량이다. 사건이 발생하면 주변 CCTV를 수집해 용의자의 동선, 인상착의를 파악하는 것은 필수적이다. 그러나 저장공간 확보를 위해 자동으로 삭제되거나 고장 등으로 인해 실체적 진실을 확인하기 어려운 경우도 종종 발생한다. 제조사별 획득방법을 숙지하고 조작을 위한 사전정보를 파악해 영상을 분석, 복구해내는 것이 필요하다. 즉, 영상을 추출하고 수동으로 복원, 재조립할 수 있는지를 평가한다.

'침해사고포렌식'(Incident Response Forensics) 역량군은 네트워크와 악성코드 등 정보통신망 침해 흔적에 대한 분석역량이다. 해킹, 분산 서비스 거부(DDoS), 랜섬웨어 등을 통해 정보통신망의 기밀성, 무결성, 가용성을 침해하는 범죄를 대응하기 위해 필요하다. 네트워크를 침투하거나 악성코드를 유포하였을 경우, 정적·동적분석을 통해 피해 범위와 악성 행위를 분석하는 기술이 요구된다. 즉, 네트워크에 대한 이론적 지식을 기반으로 공격개요를 파악하고 악성코드에 대한 세부적인 기능을 분석할 수 있는지를 평가한다.

'데이터베이스포렌식'(DB Forensics) 역량군은 데이터베이스에서 범죄혐의와 관련된 데이터를 추출, 분석할 수 있는 역량을 말한다. 분석관은 데이터베이스와 질의문(Query)을 통해 통신하고 관련 있는 정보를 추출, 복원할 수 있어야 한다. 즉, 이론적 지식을 기반으로 삭제된 레코드를 복원해 정보를 수집, 분석할 수 있는지를 평가한다.

'임베디드포렌식(Embedded Forensics)' 역량군은 임베디드(IoT를 포함) 기기에서 데이터를 수집하고 혐의를 입증하는 데 필요한 정보를 복구, 분석할 수 있는 역량이다. 임베디드 기기는 휴대용 기기와 유사한 형태를 갖고 있으나 전형화된 분석 솔루션이 없기 때문에 칩오프 등 물리적인 복원이나 자체적인 소스코드를 개발해 활용하는 기술이 요구되기도 한다. 즉, 기계적, 전자적 특성을 기반으로 하드웨어의 특성과 시스템의 구조를 파악해 증거를 추출, 분석할 수 있는지를 평가한다.

'클라우드포렌식'(Cloud Forensics) 역량군은 클라이언트와 서비스 제공자의 인프라에 존재하는 데이터를 수집, 분석할 수 있는 역량을 말한다. 클라우드 컴퓨팅 서비스가 업무에 활용되고 웹하드 업체 등이 등장하면서 클라우드 분석기술이 요구되고 있다. 방대한 자료 중에서 사건과 관련 있는 자료를 추출, 복원, 수집해내는 역량이 필요해지고 있다. 또한 로그분석을 통해 로그인한 계정, 업로드한 계정 등 사람을 추적하는 것도 중요하다. 즉, 다양한 서비스의 구조를 파악해 데이터를 수집할 수 있는지, 접근 계정을 추적하고 접속한 기기, 위치 등의 사전정보를 파악할 수 있는지를 평가한다.

4.2 디지털증거분석관 잠정 역량모델 타당성 검증

4.2.1 1차 델파이 조사 결과

역량군에 대한 내용타당도는 .73~1.00으로 모두 분석기준을 충족하였다. 역량명에 대한 내용타당도에서도 .87~1.00으로 기준을 충족하였다. 다만, 역량정의 및 행동지표 중에서 서술형 피드백으로 제시된 전문가 의견을 반영하여 5건을 수정하고 1건을 삭제하였다. 전체 역량군을 수준별로 구분할 필요가 있다는 전문가 의견이 공통으로 제시되었다. 이를 반영해 기초-필수 역량군은 모든 디지털증거분석관이 갖추어야 할 역량, 전문 역량군은 시도청별 수요 상황에 맞추어 개발 혹은 요구가 있을 수 있는 역량으로 역량군별 수준을 구분하였다.〈표 5〉

특히, 기초-필수는 역량요소도 분석관을 채용·선발 시 기준으로 활용할 수 있도록 선정하였다.

4.2.2 2차 델파이 조사 결과

1차 델파이 조사결과를 반영하여 수정된 잠정 역량모델에 대한 2차 델파이 조사결과에서 역량군에 대한 내용타당도는 .78~.89로 모두 분석기준을 초과하였고 평균, 수렴도, 합의도, 안정도 등 분석결과도 기준을 충족하였다.

Table 5. Level of Digital Evidence Examiner by Competency Cluster

DIV	Competency Cluster				
Professional	Incident Response Forensics	Video Forensics	Embedded(IoT) Forensics	DB Forensics	Cloud Forensics
Essential	Disk Forensics		Mobile Forensics		
Basic	Digital Forensic Theory		Digital evidence collection & management		

Table 6. Results of 1st/ 2nd Delphi on Competency Elements

Competency Cluster	Name	1st Delphi (CVR)	2nd Delphi					
			CVR	Mean	Standard Deviation	Convergence	Consensus	Stability
Digital Forensics Theory	Securing Integrity	1.00	1.00	4.89	0.32	0	1.00	0.07
	Create Image	1.00	1.00	4.83	0.38	0	1.00	0.08
	File System	1.00	0.89	4.67	0.77	0.13	0.95	0.16
	Timeline Analysis	1.00	1.00	4.89	0.32	0	1.00	0.07
	File Analysis	1.00	1.00	4.78	0.43	0.13	0.95	0.09
	Encryption & Decryption	1.00	0.78	4.53	0.70	0.50	0.80	0.15
Digital evidence collection & management	on-site digital evidence collection	1.00	1.00	4.83	0.38	0	1.00	0.08
	Lab management	1.00	0.89	4.83	0.51	0	1.00	0.11
	Evidentiary testimony	1.00	1.00	4.78	0.43	0.13	0.95	0.09
Disk Forensics	Acquisition of disk	1.00	0.89	4.72	0.57	0.13	0.95	0.12
	Analysis of disk	1.00	1.00	4.89	0.32	0	1.00	0.07
Mobile Forensics	Acquisition of mobile	1.00	0.89	4.83	0.51	0	1.00	0.11
	Analysis of mobile	1.00	0.89	4.78	0.55	0	1.00	0.11
Incident Response Forensics	Acquisition of network	1.00	0.89	4.56	0.78	0.50	0.80	0.17
	Analysis of network	1.00	0.89	4.61	0.78	0.50	0.80	0.17
	Malicious code Acquisition	1.00	1.00	4.72	0.46	0.50	0.80	0.10
	Malicious code Analysis	1.00	1.00	4.72	0.46	0.50	0.80	0.10
Video Forensics	Analysis of video	1.00	0.89	4.67	0.59	0.50	0.80	0.13
Embedded (IoT) Forensics	Embedded(IoT) Basics	1.00	0.89	4.67	0.59	0.50	0.80	0.13
	Acqusition of embedded(IoT)	0.87	0.67	4.22	0.73	0.50	0.75	0.17
	Analysis embedded(IoT)	1.00	0.78	4.39	0.70	0.50	0.78	0.16
DB Forensics	Acquisition of DB	1.00	0.89	4.67	0.59	0.50	0.80	0.13
	Analysis of disk	1.00	0.89	4.67	0.59	0.50	0.80	0.13
Cloud Forensics	Acquisition of cloud	1.00	0.89	4.67	0.59	0.50	0.80	0.13
	Analysis of cloud	1.00	0.89	4.72	0.57	0.13	0.95	0.12

'디지털포렌식 이론' 역량군의 표준편차가 분석기준인 .8을 초과하였으나, 다른 결과는 모두 기준을 충족해 분석관의 역량군으로 적절하다고 판단하였다. 1차 델파이 조사에서 수정한 역량군별 위계 설정에 대해 CVR은 1.00으로 전문가 패널 모두 이와 같은 위계에 동의하는 것을 확인하여(M=4.56, SD=.51, 수렴도=.50, 합의도=.80, 안정도=.11) 적절하다고 판단하였다.

수정된 잠정 역량모델의 각 역량에 대한 2차 델파이 분석결과, 역량별 CVR은 .67~1.00으로 모두 분석기준을 충족하였으며, 평균, 표준편차, 수렴도, 합의도, 안정도 등 모든 지표에서 기준을 충족하는 것으로 나타나 분석관의 역량으로 적절하다고 판단하였다.〈표 6〉 따라서 총 9개 역량군에서 25개 역량이 도출되었다. 도출된 역량군, 역량명 및 역량정의와 행동지표는 서술형 응답으로 제시된 전문가 의견을 반영해 최종적으로 확정하였다.〈표 7〉

Table 7. Final Digital Evidence Examiner Competency Evaluation Model

Cluster	Name	Competency Definitions	Behavioral Metric
Digital Forensic Theory	Securing Integrity	· Secure the technical integrity of digital evidence to prove that there has been no alteration of the original state.	· Enable to write-blocking · Generate and verify the hash values
	Create Image	· Understand the characteristics of digital evidence and acquire the duplicated data.	· Perform imaging · Create a hard-copy
	File System	· Explain the concept of file system(operating system) and recover it.	· Explain the concept of file system · Restore file system · Explain OS(Operating System)
	Timeline Analysis	· Confirm the temporal sequence of cases andevidence destruction status through timeline analysis.	· Verify the configured timestamp on the target device and confirm the processing time of files, etc.
	File Analysis	· Examine fabrication and manipulation of file by verifying their metadata and structure.	· Confirm fabrication and manipulation of files, etc.
	Encryption & Decryption	· Identify encrypted files and acquire data by decrypting them.	· Utilize basics related encryption and decryption
Digital Evidence Collection & Management	on-site digital evidence collection	· Obtain a warrant that meets the digital evidence to be seized, and collect the digital evidence in accordance with the procedures within the scope of the warrant or voluntary submission.	· Establish advance plan for collecting digital evidence. · Manage the site where digital evidence is seized and collect on-site evidence. · Lawfully export and manage media collected from the site.
	Lab forensic management	· Conduct digital evidence collection and analysis by adhering to the fundamental principles and legal procedure.	· Collect, analyze, and manage requested item in accordance with legal procedure.
	Evidentiary testimony	· Identify the issues in dispute in court, and testify the processes and results of the analysis.	· Provide evidentiary testimony related to the analysis of digital evidence in the cases.
Disk Forensics	Acquisition of disk	· Acquire data from a computer and handle exceptional situations that may occur.	· Acquire data based on characteristics and condition of each disk medium. · Collect volatile data(memory dump).
	Analysis of disk	· Recover and search data, and analyze it by integrating the artifact's path and relationships.	· Recover deleted files. · Efficiently search for data. · Explore the connection traces of external storage media and analyze them. · Analyze artifacts. · Analyze emails. · Analyze PC messengers. · Confirm traces of data tampering or deletion.
Mobile Forensic	Acquisition of mobile	· Acquire data from a mobile device and handle exceptional situations that may occur.	· Collect data in accordance with the characteristics and condition of each mobile medium. · Understand and customize the function of dedicated programs. · Understand and utilize the mobile operaing system and file storage structure. · Verify the results automatically analyzed by programs. · Manually analyze items not properly analyzed by programs. · Detect the concealment, destruction, or deletion of evidence.
		· Analyze mobile data by utilizing dedicated software, otherwise manually recover, decode, and parse any remaining data.	
Incident Response Forensics	Acquisition of network	· Understand network structure and operation principles, and collect traffic and data.	· Understand and utilize the network operation principles. · Acquire network information.
	Analysis of network	· Analyze network data	· Collect data through log analysis. · Analyze traffic. · Analyze network systems.
Video Forensics	Analysis of video data	· Convert video stored in video devices such as CCTV, black boxes, and restore deleted videos.	· Understand the preliminary information for analysis. · Select and utilize appropriate methods for file recovery and conversion. · Recover and assemble frames.

Cluster	Name	Competency Definitions	Behavioral Metric
Embedded Forensics	Embedded (IoT) Basics	· Understand the characteristics of embedded(IoT) devices and systems, and explain the fundamental knowledge required for hardware and software forensics.	· Explain the principles of the electrical operation of devices and communication. · Understand embedded(IoT) devices and utilize them for hard forensics. · Understand embedded(IoT) devices and utilize them for software forensics.
	Acquisition of embedded (IoT)	· Collect embedded(IoT) data using chip-off equipment and interfaces, or circumvented using vulnerabilities or interconnected devices.	· Collect embedded(IoT) data depending on the type of interfaces · Extract data by chip-off from flash memory
	Analysis embedded (IoT)	· Identify data stored on embedded(IoT) devices, and recover, decode, and parse relevant data.	· Analyze embedded(IoT) data · Analyze software of embedded(IoT) devices
DB Forensics	Acquisition of DB	· Understand the characteristics based on DB data types and collect them.	· Understand the structure of DB by types · Collect data from DB
	Analysis of DB	· Restore DB data and analysis it.	· Recover DB data · Analyze DB
Cloud Forensics	Acquisition of cloud	· Understand the concept of cloud computing and collect data remotely.	· Explain the concept of cloud computing · Collect data on cloud access and usage history
	Analysis of cloud	· Analyze cloud data	· Analyze data collected from the cloud

V. 결 론

디지털증거를 법정에서 유죄를 판단하기 위한 증거로 사용하기 위해 분석관에게 무결성 입증을 비롯하여 다양한 전문성이 요구되고 있다[4]. 분석관은 처리의 각 단계에서 업무처리자 변동 등의 이력을 관리해야 하고 자신이 수행한 모든 과정이 적절했다는 것을 입증해야 한다[8].

본 연구는 디지털증거 분석 업무를 수행하는 전문가 18명을 대상으로 전문가 FGI, 델파이 조사를 활용해 총 9개 역량군, 25개 역량으로 역량모델을 정의하였다. 이를 위해 문헌연구와 전문가 FGI 결과를 종합하여 잠정 역량모델을 도출하였고 2회의 델파이 조사를 통해 타당성을 검증하였다. 마지막으로 델파이 결과와 서술형으로 응답한 전문가의 의견을 종합하여 최종 역량모델을 규명하였다. 분석관에게 필요한 역량을 현직자의 의견을 반영해 디지털증거 분석에 특화된 역량모델을 개발하였다는 점에서 의미가 있다. 다만, 인공지능, 가상자산, 딥페이크 등 새로운 매체가 지속적으로 출시되고 있어 해당 시점에서 필요한 역량군별 우선순위는 계속 변동할 수 밖에 없다. 이에 맞춰 필수와 심화 역량군을 꾸준히 수정·보완는 것이 필요하다. 그러나 분석관 역량정의와 분류체계를 마련하는 연구의 시발점으로서 분석관의 선발, 분석업무, 교육훈련, 업무평가, 숙련도 평가 등에 기초자료로 활용될 수 있을 것이다. 나아가, 분석관의 전문성을 인정받기 위한 평가모델로 활용되기를 기대한다.

References

[1] Hyun-ju Kim, Eun-sun Choi, and Nam-je Park, "Demonstration of the curriculum to strengthen digital forensics capabilities required for field police officers," Journal of Next-generation Convergence Technology Association, 6(3), pp. 483-493, Mar. 2022.

[2] Hyun-seok Yoon, "A study on the seizure and search problems of smart phone digital evidence and improvement measures," Korean Society of Computer Information, 28(2), pp. 187-188, Jul. 2020.

[3] The JoongAng, "Shocking Actions by Cho Joo-bin, even the Prosecutor was Surprised," The prosecutor was also surprised https://www.joongang.co.kr/article/25112965#home (20 JAN, 2023 confirmed)

[4] Yang-sub Kwon, "A study case law reflections on the admissibility of digital evidence," Journal of The Korea Onstitute of Information Security and Cryptology, 26(5), pp. 44-53, Jun. 2016.

[5] Ministry of Trade, Industry and Energy Report, Birth of the World's First International Accreditation Body in the Field of Digital Forensics, http://www.

motie.go.kr/motie/gov3.0/gov_openinfo/sajun/bbs/bbsView.do?bbs_seq_n=163119&bbs_cd_n=81 (20 JAN, 2023 confirmed)

[6] M. Dalal and M. Juneja, "Steganography and steganalysis (in digital forensics): a cybersecurity guide," Multimedia Tools and Applications, vol. 80, no. 4, pp. 5723 - 5771, Feb. 2021.

[7] Jong-min Kim, Kyung-ho Choi, and Kui-nam Kim, "Research about the development of education courses for nurturing digital forensic experts," Jouranl of Information and Security, 12(5) pp. 79 - 85, Oct. 2012.

[8] Hae-jung Yun, Seung-yong Lee, and Choong-cheang Lee, "Deriving priorities of competences required for digital forensic experts using AHP," The Journal of Society for e-Business Studies, 22(1), pp. 107 - 122, Feb. 2017.

[9] Gi-bum Kim, Ki-sik Chang, Yoon-sik Jang, Sang-jin Lee, and Jong-in Lim, "A study on developing certificate program model for digital forensic examiner," Journal of digital forensics, 2(1), pp. 29 - 51, Nov. 2008.

[10] Yoon-jung Lee, Yun-cheol Baek, Sung-hoon Son, and Jin-oo Joung, "On development of curriculum for digital forensic professionals," Journal of Digital Forensics, 3(2), pp. 89 - 105, Nov. 2009.

[11] Hee-il Park, Jong-sung Yoon, and Sang-jin Lee, "A study on development of digital forensic capability evaluation indices," Journal of the Korea Institute of Information Security and Cryptology, 25(5), pp. 1153 - 1166, Oct. 2015.

[12] Nam-myung Kim and Hun-yeong Kwon, "A study on how to improve digital forensic reliability and expertise of the Police," The Journal of Police Policies, 36(1), pp. 313-342, Mar. 2022.

[13] Ji-ho Shin and Nak-bum Choi, "A study on improving of digital forensic organization and work procedures in police," The Journal of Police Science, 16 (3), pp. 231 - 262, Sep. 2016.

[14] L.M. Spencer and S.M. Spencer, Competence at work: models for superior performance, 1st Ed., Wiley, Apr. 1993.

[15] Sun-young Pyo, Se-eun Hong, and Je-yong Jung, "A study of job competency of dialogue police in Korea," The Journal of Police Science, 22(2), pp. 29 - 66, Jun. 2022.

[16] Jun-seon Jeong, "The competency model development for police in workplace training," Master's Thesis, Hanyang Cyber University Graduate School of Education Information, Aug. 2015.

[17] A.S. Raelin and J.A. Cooledge, "From generic to organic competencies," Human Resource Planning, vol. 18, no.3, pp. 24 - 33, Apr. 1995.

[18] Joon-woo Shin, "A study on digital forensic human training method," Journal of the Korea Institute Of Information and Communication Engineering, 18 (4), pp. 779-789, Apr. 2014.

[19] Hyun-dae Na, Chang-jae Kim, and Nam-yung Lee, "A Study on designing an undergraduate curriculum in digital forensics per stages for developing human resource," The Journal of Korean Association of Computer Education, 17(3), pp. 75-84, May. 2014.

[20] Hee-bong Kim et al., HRD Research Methodology Guide: Starting Point of Research and Practice, 1st Ed., Park Young's Story, May. 2022.

[21] J.W. Murry and J.O. Hammons, "Delphi: a versatile methodology for conducting qualitative research," The Review of Higher Education, vol. 18, no. 4, pp. 423 - 436, summer 1995

[22] R. Lepsinger and A.D. Lucia, The art and science of competency models: Pinpointing critical success factors in organizations, 1st Ed., Pfeiffer, Mar. 1999.

[23] Yon-ho Park, "A reconsideration of competency: overcoming the confusion in understanding and applying the competency concept," Lifelong Education and HRD Research, 14(3), pp. 89 - 113, Jul. 2018.

[24] L.B. Mokkink et al., "The COSMIN study reached international consensus on taxonomy, terminology, and definitions of measurement properties for health-related patient-reported outcomes," J Clin Epidemiol, vol. 63, no. 7, pp. 737 - 745, Jul. 2010.

[25] C. Ayre and A.J. Scally, "Critical values for lawshe's content validity vatio: revisiting the original methods of calculation," Measurement and Evaluation in Counseling and Development, vol. 47, no. 1, pp. 79 - 86, Jan. 2014

[26] Kyng-a Seo and Jong-won Jung, "Developing a parent education program for improving empathy ability applying the delphi technique," Korean Journal of Psychodrama, 23(1), pp. 17 - 35, Jun. 2020.

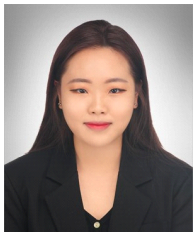
[27] Chun-ju Kim, Hyeon-ah Jo, and Ji-hoon Song, "Exploring the competencies of Korean language career teachers: focusingon on the 'project to support the overseas practicum of Korean language pre-service teachers'," Journal of Learner-Centered Curriculum and Instruction, 23(1), pp. 97 - 116, Jan. 2023.

[28] Na-yeon Kwak, Choong-cheang Lee, Yun-ho Maeng, Bang-ho Cho, and Sang-eun Lee, "A meta study on trends of digital forensic research in Korea," Informatization Policy, 24(3), pp. 91 - 107, Sep. 2017.

[29] Galaxy Computer Services, Inc. v. Baker, 325 B.R. 544-E.D.Va.2005.

[30] Krause v. State, 243 S.W.3d 95(Tex.App. Houston 1st Dist. 2007.

〈저자소개〉



오 소 정 (Oh SoJung) 학생회원
2019년 2월: 상명대학교 컴퓨터과학과 졸업
2020년 3월~2022년 8월: 성균관대학교 과학수사학과 석사(디지털포렌식전공)
2020년 7월~현재: (사)한국디지털포렌식학회 간사
2023년 2월~현재: 성균관대학교 과학수사학과 박사과정
〈관심분야〉 디지털포렌식, 사이버범죄수사, 모바일포렌식, 다크웹추적 등

정 준 선 (Jeong JunSeon) 정회원
2001년 2월: 경찰대학 법학과 졸업
2015년 8월: 한양사이버대학교 교육정보대학원 교육학석사
2021년 3월~현재: 한양대학교 교육공학과 박사과정 수료
2018년 1월~현재: 경찰대학 경찰학과 교수
〈관심분야〉 역량모델링, 역량기반 교육과정 설계, 교육과정 평가, 조직사회화 등

조 은 별 (Cho EunByul) 정회원
2009년 2월: 경찰대 법학과 졸업
2012년 2월 서울대 형사법 석사
2021년 8월: 서울대 형사법 박사
2015년 12월~2023년 2월: 서울경찰청 디지털포렌식계 분석팀장
2023년 2월~현재: 경찰대학 경찰학과 교수
〈관심분야〉 디지털포렌식, 디지털증거법, 사이버범죄수사 등

김 기 범 (Kim GiBum) 종신회원
1997년 2월: 경찰대학 행정학과 졸업
2009년 2월: 고려대학교 정보보호대학원 공학석사
2017년 2월: 고려대학교 정보보호대학원 공학박사
2014년~2020년: 경찰대학 경찰학과 교수요원
2020년 3월~현재: 성균관대학교 과학수사학과(디지털포렌식) 부교수
〈관심분야〉 경찰, 디지털포렌식, 사이버범죄수사, 정보보호, 국제개발협력 등