Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.3, Jun. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.3.417

무결성 향상을 위한 모바일 포렌식 모델 연구

김 영 준,[1†] 김 완 주,[2] 임 재 성[2‡]
[1,2]아주대학교 (대학원생, 교수)

A Study the Mobile Forensics Model for Improving Integrity

Young-june Kim,[1†] Wan-ju Kim,[2] Jae-sung Lim[2‡]
[1,2]Ajou University(Graduate student, Professor)

요 약

정보통신기술의 비약적인 발전과 함께 모바일 장치는 우리 생활에 있어 필수적인 도구가 되었다. 모바일 장치는 대부분의 시간을 사용자와 함께 하면서 개인 정보 관리(PIM) 기능과 동시에 데이터를 축적하기 때문에 범죄 증명에 있어 중요한 증거 자료로 활용된다. 모바일 포렌식은 모바일 기기로부터 디지털 증거를 획득하는 절차로 기타 증거와 동일하게 적법절차에 따라 수집 및 분석이 이루어져야하며, 변조 및 삭제가 용이한 측면을 가지고 있어 증거의 무결성 입증이 필수적이다. 또한, 증거의 채택은 법관의 자유심증주의에 의존하고 있어 일반화된 절차 제시가 절실하다. 본 논문에서는 절차의 일반화를 통해 무결성을 보장받을 수 있는 모바일 포렌식 모델을 제시하였다. 제시된 모바일 포렌식 모델을 통해 증거의 신뢰성과 진정성을 확보함으로써 법관의 심증형성에 기여할 수 있을 것으로 기대된다.

ABSTRACT

With the rapid development of information and communication technology, mobile devices have become an essential tool in our lives. Mobile devices are used as important evidence in criminal proof, as they accumulate data simultaneously with PIM functions while working with users most of the time. The mobile forensics is a procedure for obtaining digital evidence from mobile devices and should be collected and analyzed in accordance with due process, just like other evidence, and the integrity of the evidence is essential because it has aspects that are easy to manipulate and delete. Also, the adoption of evidence relies on the judges' liberalism, which necessitates the presentation of generalized procedures. In this paper, a mobile forensics model is presented to ensure integrity through the generalization of procedures. It is expected that the proposed mobile forensics model will contribute to the formation of judges by ensuring the reliability and authenticity of evidence.

Keywords: Mobile Forensic, Digital Evidence, Forensic Model, Integrity

I. 서 론

휴대폰, 태블릿 등 모바일 장치는 급속한 성장과 발전으로 기존의 데스크탑 컴퓨터와 유사한 수준의 작업 수행여건을 보장하여 오늘날 개인 및 업무에 필수적인 도구로 사용되고 있다[1]. 전 세계적으로 모바일 장치의 활용이 확장됨에 따라 이를 활용한 사이버범죄 활동도 크게 증가하고 있다[2]. 모바일 장치는 이메일(Email), 모바일 메신저(MMS : Media Messaging Service), 소셜 네트워크 서비스(SNS : Short Message Service), 위치기반 서비스, 웹 브라우징 등 여러 기능을 사용자에게 제공하고 소유자 및 장치로 수행 된 활동에 대한 상당한

Received(03. 09. 2020), Accepted(04. 21. 2020)
† 주저자, storesomeday@ajou.ac.kr
‡ 교신저자, jaslim@ajou.ac.kr(Corresponding author)

양의 정보를 축적하게 되면서 모든 일상이 기록되어 디지털 데이터 형식으로 기기에 기록되게 되었다[3]. 특히, 기기에 저장된 네트워크 전송 패킷 및 로그기록 등의 데이터는 법 집행 기관 또는 기타 보안 담당자에게 각종 범죄현장의 중요 근거자료로 활용되는 등 범죄 증명의 중요한 디지털 증거로 사용되고 있다[4].

모바일 기기로부터 디지털 증거를 획득하는 일련의 과정을 모바일 포렌식이라고 하며[5], 다수의 법정에서 디지털 증거가 핵심 증거로 채택하고 있다[6]. 그러나, 모든 디지털 증거가 증거로서의 효력을 발휘하는 것은 아니다. 디지털 증거는 다른 증거와는 다르게 전자적인 특성을 가지고 있어 변조되거나 삭제되는 등 변형이 쉬워 무결성이 확보 되지 않으면 증거로서의 효력을 잃게 된다[7].

대부분의 공공기관 및 수사기관은 무결성 확보를 위해 미국 국립표준기술연구소(NIST)의 'Guidelines on Mobile Device Forensics'와 한국정보통신기술협회(TTA)의 'Guidelines on Cellular Phone Forensics'에서 제시한 모바일 포렌식 절차를 준용하고 있다.

하지만 NIST는 2007년 5월 30일, 처음으로 'Guidelines on Cell Phone Forensics'을 출판한 이후 7년이 지난 2014년 5월, 개정 버전인 'Guidelines on Mobile Device Forensics'을 출판하였고[5] TTA는 2007년 12월 26일, 'Guidelines on Cellular Phone Forensics'을 출판하여[8] 수년 간 개정되어 오고 있지 않아 오늘날 모바일 포렌식 절차를 수행함에 있어 무결성을 보장받지 못하는 절차적 한계를 보인다.

최근에 디지털 증거가 법정에 자주 제출되어 증거로서 효력을 인정받는 사례가 종종 있어왔지만 무결성 입증의 한계로 증거능력을 인정받지 못하거나 추가 입증을 위해 전문기관의 분석 의뢰 등의 과정을 거치는 경우 역시 발생하고 있으며, 증거의 채택은 법관의 자유심증주의에 의존하고 있어 무결성을 보장받을 수 있는 표준화된 절차 제시가 필요하다. 기존의 다양한 연구에서는 부분적 절차 보완의 노력을 해왔지만 무결성 보장을 위한 체계적인 절차 제시가 미흡한 실정이다[9][10][11][12][13].

따라서 본 논문에서는 모바일 포렌식 절차를 수행함에 있어 무결성 향상을 위한 모델을 제시함으로써, 디지털 증거의 신뢰성과 진정성 확보를 통한 법정에서의 법관 심증형성 및 증거효력 입증에 크게 기여할 것으로 기대된다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 모바일 포렌식 개념과 디지털 증거 특징, 표준 가이드라인에 대한 기존 연구를 제시하고 Ⅲ장에서는 무결성 향상을 위한 새로운 모바일 포렌식 모델을 제안한다. Ⅳ장에서는 Ⅲ장에서 제안한 모바일 포렌식 모델에 대한 기존의 표준 가이드라인과의 비교및 실제 대법원 판례에 입각한 사례연구를 통해 제안한 모델의 효과를 검증하고 Ⅴ장에서는 본 연구의 기대효과와 향후 연구 방향을 제시하며 결론을 맺는다.

Ⅱ. 관련연구

2.1 모바일 포렌식 개념 및 디지털 증거의 특징

전통적으로 포렌식 개념은 법의학 분야에서 지문, 모발, 족적, DNA 감식 등에 주로 이용되었다. 그러나 최근 다양한 디지털기기들의 활용으로 포렌식 개념은 물리적인 형태의 증거뿐만 아니라 전자적 증거를 다루는 디지털 분야로 점차 확대되고 있다[14]. 그중 모바일 포렌식은 디지털 포렌식 분야의 하나로 모바일 기기에 기억된 전자적 정보를 정확히 식별하여 수집하고, 보존, 분석을 통해 관련된 정보를 특정하여 법정에 증거로 제출하고, 언제든지 검증이 가능한 형태로 자료를 준비하는 절차를 의미한다[15].

따라서 모바일 포렌식은 정당성, 무결성, 연계보관성, 재현성, 신속성의 디지털 포렌식 조사의 5가지 일반 원칙을 준수하는 가운데 디지털 증거를 확보하는 노력을 기울여야 한다. 디지털 증거의 특징은 다음과 같다[16].

첫째, 비가시성과 비가독성을 가진다. 눈에 보이지 않는 0과 1의 조합인 디지털 형태로 저장되어 있어 그 자체로는 육안 식별이 불가능하여 일정한 변환 절차를 거쳐 모니터 화면으로 출력되거나 프린터를 통하여 인쇄된 형태로 출력되어야 한다.

둘째, 취약성이 존재한다. 오류에 의한 손상이나 의도적인 변조가 쉬우며, 변조 사실을 찾아내기 어려운 취약성이 존재한다.

셋째, 복제 용이성이 있다.

넷째, 데이터의 대량성을 가진다.

다섯째, 휘발성이 있다.

여섯째, 전문성이 요구된다. 디지털 증거의 압수·수집·분석에 전문적인 포렌식 기술이 사용되므로 포렌식 전문가가 필요하며, 전문성의 부재는 디지털 증

거에 대한 신뢰성 문제를 야기 하게 된다.

2.2 NIST, TTA의 표준 가이드라인

본 연구에서는 모바일 포렌식 모델 개발을 위해 국내·외에서 적용되는 가장 보편적이고 적용 범위가 넓은 NIST, TTA의 표준 가이드라인을 기준으로 하였으며, 대검찰청 디지털증거 압수수색 모델 등 수사기관 자체적으로 한정되어 있는 표준 모델들은 본 연구 범위에 포함하지 않았다.

2.2.1 NIST 가이드라인

NIST의 'Guidelines on Mobile Device Forensics'은 기관에서 모바일 장치를 다루기 위한 적절한 정책과 절차를 발전시키고 포렌식 전문가가 포렌식 도구를 활용하여 핵심의 디지털 증거를 추출하여 수사에 활용하도록 하는 표준 절차를 제시하였다.

NIST 가이드라인은 Fig. 1.과 같이 총 4가지 절차로 구분된다.

디지털 증거의 보존단계((1))는 장치 및 이동식 미디어에 있는 데이터의 내용을 변경하거나 변경하지 않고 재산 관리를 안전하게 유지하도록 한다. 획득단계((2))는 모바일 장치 및 관련 미디어에서 정보를 이미징하거나 다른 방식으로 얻는 과정을 의미한다. 검사 및 분석 단계((3))는 포렌식 전문가에 의해 포렌식 툴과 같은 과학적 방법을 적용, 사건과 직접적인 데이터를 검사 및 분석하여 결과를 도출한다. 보고서 단계((4))는 조사 할 때 취한 모든 단계와 결론에 대한 자세한 요약을 준비하는 과정으로 모든 행동과 관찰에 대한 주의 깊은 기록을 유지하고, 시험 및 시험 결과를 설명하고, 데이터에서 도출된 추론을 설명하는 방식으로 작성하도록 한다.

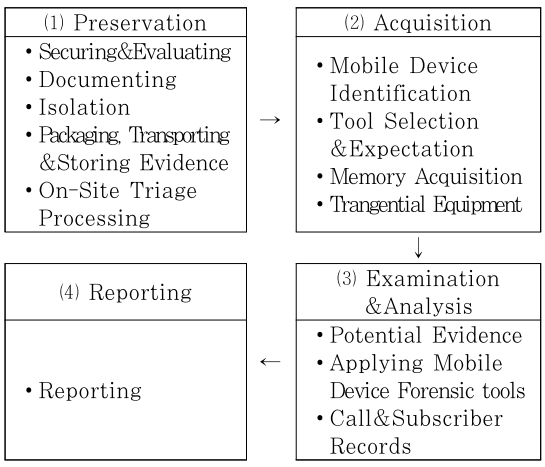

Fig. 1. Guidelines on Mobile Device Forensics Procedure

본 가이드라인은 4가지의 단계 - 디지털 보존, 획득, 검사 및 분석, 보고서 - 를 제시하였지만 다음과 같은 한계를 가진다.

첫째, 디지털 증거의 특징상 사전 포렌식 절차를 수행하기 전에 법적 기준 검토와 포렌식 전문가에 대한 전문성 확보 등의 증거효력을 확보하고 무결성을 보장받기 위한 사전준비가 필요하지만 절차적으로 부재하다.

둘째, 단계별 절차가 복합적으로 구성되어 있어 디지털 증거의 일반원칙을 준용하기 어렵기 때문에 각 단계에 포함되어 있는 세부단계를 분리하고 재정립하는 과정이 필요하다.

2.2.2 TTA 가이드라인

TTA 'Guidelines on Cellular Phone Forensics'은 휴대폰 내에 저장되어 있는 디지털 증거에 관한 절차와 준수 사항으로 수집, 분석, 보관의 과정이 적법한 절차로 이루어질 수 있도록 표준 가이드라인을 통해 증거의 무결성을 보장함과 동시에 적법한 절차를 통해 디지털 증거물을 취급 할 수 있는 방안 및 조사 행위를 정립하여 제시한다.

TTA 가이드라인은 Fig. 2.과 같이 총 6가지 절차로 구분된다.

수사준비단계((1))는 증거의 수집 및 분석을 위한 포렌식 도구의 구비 및 수사관에 대한 교육을 포함한다. 초기대응단계((2))는 사건 현장을 보존하고 기록하며, 휴대폰에 저장되어 있는 디지털 증거를 물리적으로 수집하고 수집된 증거를 이용하여 수사를 진행한다. 증거수집단계((3))는 휴대폰의 상태 및 휴대폰에 대한 포렌식 하드웨어, 소프트웨어 도구의 지원 여부에 따라 적합한 수집 방법을 적용하여 디지털 증거를 수집한다. 포장 운송 및 보관단계((4))는 디지털 증거물이 포장 운송 및 보관단계에서 손상되지 않도록 쓰기방지 조치를 취하고, 정전기 팩을 사용하여 외부의 전자기력으로 인한 손실을 예방한다.

조사 및 분석단계((5))는 수집한 증거들을 토대로 사건과 직접적으로 관련이 있는 증거를 추출한다. 보고서 단계((6))는 결과보고서는 수정이 불가능한 문서

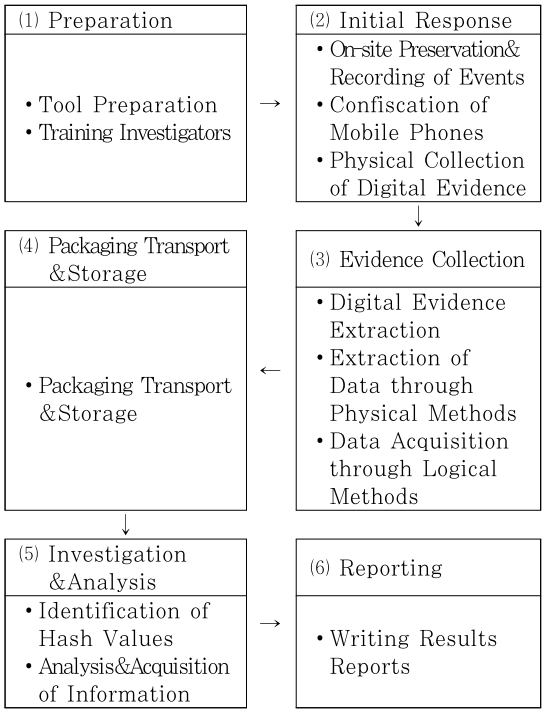

Fig. 2. Guidelines on Cellular Phone Forensics Procedure

자료 형태로 부본을 작성하여 관련 사건의 재판 종결 시 또는 공소시효 만료 시 까지 증거보관실에 보관하며, 증거물 수집, 보관, 분석 등의 과정을 6하 원칙에 따라 명백하고 객관성 있게 작성하도록 한다.

본 가이드라인은 6가지 단계 - 수사준비, 초기대응, 증거수집, 포장 운송 및 보관, 조사 및 분석, 보고서 - 를 제시하였지만 다음과 같은 한계를 가진다.

첫째, 이동전화에 한정되어 있어 포렌식 적용 범위가 좁으며, 이동전화만을 식별하기 때문에 어떠한 기기를 대상으로 특정하여 선별할 것인지에 대한 절차구성이 제외되어 있다.

둘째, 증거의 포장, 운송, 저장단계는 절차 수행방법에 관한 유의사항만을 단순히 열거하고 있고 단일 단계로서 구분 하였지만 내용상 다수의 단계에 절차적으로 영향을 미쳐 혼선을 야기할만한 부분을 포함하고 있다.

NIST, TTA 가이드라인의 공통사항으로 증거로부터 데이터를 추출하는 방식이 과거의 기술에 머물러있어 현재의 기술에는 적용할 수 없는 데이터 획득 기법이 다수이고 사용되는 기술을 포함할만한 절차과정 역시 부재하다. 또한, 증거의 무결성 보장을 위해서는 증거의 환부·삭제·보관·열람·파기 과정이 필요하지만 제시하고 있지 않다.

III. 무결성 향상을 위한 모바일 포렌식 모델 제안

본 연구의 목적은 모바일 포렌식 절차를 수행함에 있어 증거 수집 단계부터 법정에 제출되어 증거로 채택될 때까지의 무결성 보장을 통해 디지털 증거의 효력을 보장받는 모델을 제시하는 것이다.

3.1 모바일 포렌식 모델 구성

본 연구에서는 Ⅱ장에서 모바일 포렌식 개념 및 디지털 증거의 특징, 모바일 포렌식의 대표적인 NIST, TTA의 표준 가이드라인을 통해 Fig. 3.과 같이 5가지의 단계 - 증거 압수 준비(Evidence Seizure Preparation), 증거 획득(Evidence Acquisition), 분석 및 복원(Investigation& Restoration), 보고서(Reporting), 증거 보존 및 관리(Evidence Retention&Management) - 를 도출하였다. 또한, 다음 모델은 기존의 표준 가이드라인에서 제시하고 있지 않는 주요 차별화 단계인 사전준비단계, 새로운 데이터획득 단계, 증거 검토단계 및 증거 보존 및 관리단계의 별도 구성 등을 적용한다.

3.1.1 증거 압수준비 단계

증거 압수준비 단계((1))는 증거의 신뢰성을 확보하기 위해 검증된 포렌식 도구를 준비하고 수사관의 능력 배양과 증거수집 절차 및 계획을 수립한다. 증거를 추출하기 전 기초단계로서 준비, 선별 보존, 조사 및 인식, 문서화의 세부단계를 포함한다.

준비단계는 위법 절차 없이 포렌식 절차를 진행하기 위한 포렌식 도구를 준비하고 점검 하는 것이 요구되며, 수사관은 수사전에 포렌식 도구가 신뢰성이 있는지 점검할 의무를 가진다.

조사 및 인식 단계는 디지털 증거의 수집이 수사목적을 달성하는데 필요한 최소한의 범위에서 이루어지도록 사전에 사건의 개요, 압수수색 검증 장소 및 대상, 정보 저장매체 등의 유형과 규모 등 필요한 사항을 고려한다.

선별 보존 단계는 조사 및 인식 단계를 거쳐 식별된 정보 저장매체를 피압수자 동의/협조 또는 참여인 입회하에 선별하여 보존한다. 문서화 단계는 현장 도

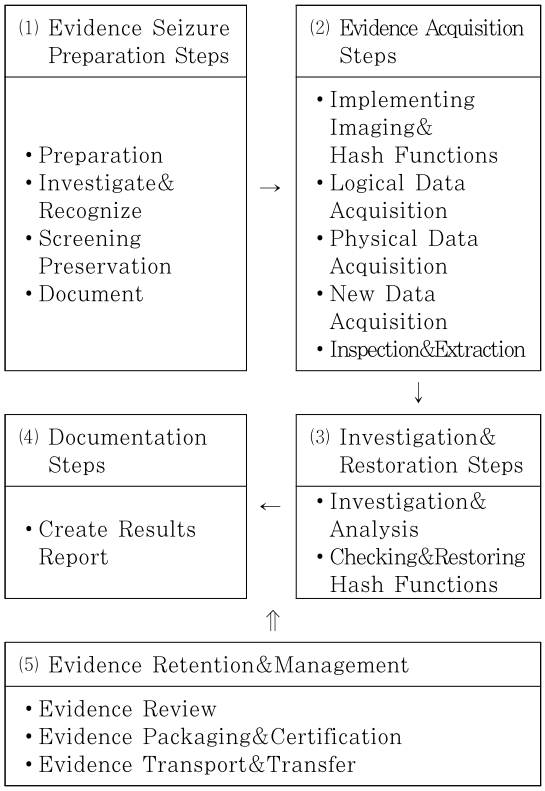

Fig. 3. Mobile Forensics Model for Improving Integrity

착 이후부터 검색대상을 선별/압수하는 과정을 녹화, 기록 등을 거쳐 증거확보가 적법한 절차에 의해 이루어졌다는 검증을 위한 보충자료의 역할을 한다.

3.1.2 증거 획득 단계

증거 획득 단계((2))는 모바일 포렌식을 통해 모바일 기기로부터 디지털 증거를 추출하는 단계로 신속성을 보장한다. 디지털 증거의 증거 수집은 모바일 기기의 상태 등을 고려한 적합한 수집 방법을 적용해야 하며, 이를 위해 이미징 및 해쉬함수 구현, 논리적인 데이터 획득, 물리적인 데이터 획득, 새로운 데이터 획득, 검사 및 추출의 세부단계로 구성한다.

이미징이 가능한 단순 저장매체와 같은 기기는 이미징 및 해쉬함수 구현단계를 통하여 데이터를 수집하고 수집된 증거에 해쉬값을 부여한다. 직접 이미징이 불가능한 모바일 기기는 물리적 방법과 논리적 방법을 통하여 데이터를 획득한다. 물리적 방법은 기기의 플래쉬 메모리를 분리하여 직접 메모리를 읽는 방법과 JTAG와 같은 표준 하드웨어 인터페이스를 이용한 방법이다. 논리적 방법은 파일전송 프로토콜을 이용한 직접 획득 방법과 제조사의 PC소프트웨어를 이용한 방법이다. 각자의 방법을 통하여 디지털 증거를 획득하는 단계를 물리적 데이터 획득단계와 논리적인 데이터 획득단계라고 한다.

새로운 데이터 획득단계는 기존의 데이터 획득기법으로는 추출하지 못하는 데이터에 관한 연구를 반영한 단계로 신규 기기의 잦은 출시와 함께 소프트웨어의 주기적인 업데이트 지원, 여러 회사에서 출시하는 모바일 기기의 OS와 소프트웨어의 다양화 등으로 보안이 강화되어 물리적 벙법과 논리적 방법을 통한 데이터 획득이 불가능한 경우 기존의 연구되어진 획득기법과 향후 연구될 획득기법을 포함한 새로운 획득단계라고 할 수 있다.

3.1.3 분석 및 복원 단계

분석 및 복원 단계((3))는 과학적인 방법으로 디지털 증거를 면밀히 살펴 법정에 제출할 수 있는 상태로 만들어주는 단계로 조사 및 분석, 해쉬함수 확인 및 복원의 세부단계를 포함하여 무결성 보장과 재현성을 증명한다.

수집된 증거를 토대로 사건과 직접적으로 관련이 있는 증거를 추출하는 조사 및 분석 단계를 거쳐 무결성의 침해 여부를 확인할 수 있는 해쉬값의 일치 여부와 데이터 복원 작업인 해쉬함수 확인 및 복원 단계를 통해 범죄의 유·무죄를 증명할 수 있는 기반을 마련한다.

3.1.4 보고서 단계

보고서 단계((4))는 분석한 데이터를 보고서 형식으로 작성하여 증거로서 법정에 제출될 수 있도록 가시성과 가독성을 확보하여 무결성을 확증하는 단계이다.

결과 보고서 작성은 수사과정에서 각각의 증거데이터 단계에 대한 상세하고 요약된 결과로 구성하며, 조사, 분석자의 모든 행동과 관찰 내역, 분석 과정 등의 내용을 명확하고 객관성 있게 6하 원칙에 따라 작성한다.

3.1.5 증거 보존 및 관리 단계

증거 보존 및 관리단계((5))는 원본증거의 연계보

관성과 무결성이 보장하기 위해 독립적인 별도의 단계로 구성하였고 증거 검토, 증거 포장 및 인증, 증거 운반 및 양도의 세부단계로 구성한다.

증거 검토단계는 본 논문에서 새로 제시한 단계로 디지털 증거가 가환부·환부·삭제되기 전에 검토를 실시하여 무결성을 보장하기 위함이다. 증거의 가환부·환부·삭제는 디지털 증거의 특성에 따라 정보저장 매체 압수, 이미징 및 복제·복사 파일 압수, 압수한 출력물로 압수형태가 달라진다.

매체 자체를 압수한 경우 법률상 권리의 객체가 되는 물건이므로 압수물의 환부 절차에 의해 환부하고 압수기관에서 복사하여 남겨진 디지털 증거는 공판 이후 보관의 필요성이 소멸하면 영구적으로 삭제하도록 한다. 이미징·하드카피·파일 복사의 방법으로 압수한 경우는 별도의 반환 절차 없이 삭제하며, 출력하여 제출한 경우는 사건 관련성이 있는 정보만을 인쇄하여 압수한 것이므로 출력물에 대해 환부요청이 있을 때에 한해 환부하고 협의 사실과 관련 없는 출력물은 파기 절차를 거치게 된다.

즉, 사건과 무관한 정보라고 판단되는 피압수자의 사생활 정보, 불필요한 데이터 등은 전부 환부·삭제된다. 이 과정을 통해 발생한 데이터의 변조는 무결성을 침해받아 더 이상 증거로서의 역할을 수행할 수 없게 된다. 그러므로 디지털의 증거의 환부·가환부·삭제 여부를 판단하는 절차는 무결성을 보장받는 상태로서의 증거 가치를 유지하는데 중요한 과정이다. 별도의 절차 없이 증거가 환부·삭제된다면 디지털 증거로서의 효력을 침해받게 되며, 재환부하여 증거를 취득하였다 하더라도 환부과정에서의 무결성을 입증하지 못한다면 경우에 따라 증거로서의 효력을 보장받지 못하는 상황이 발생하게 된다.

증거 포장 및 인증단계는 디지털 증거의 훼손을 방지하기 위해 현장에서 선별 압수한 기기 및 저장매체를 전파 차단봉투 및 차단장비를 활용하여 차단하는 과정을 의미한다. 디지털 증거의 특성상 원본 자료나 하드카피, 이미징을 거친 자료가 훼손될 가능성이 크며, 훼손은 무결성이 손상됨을 의미한다. 증거 운반 및 양도단계는 증거가 압수되어 분석을 거치는 과정에서 인수인계가 이루어지기 때문에 증거의 연계보관성을 보장하기 위해서 필요한 단계이다.

증거물 보관·이송 단계는 Fig. 4.과 같이 여러 단계와 연관되어있어 일련의 과정이 어느 한 과정에 종속된다고 보기 어렵기 때문에 증거 압수 준비 단계부터 보고서 단계까지의 공통 단계이자 독립단계로서

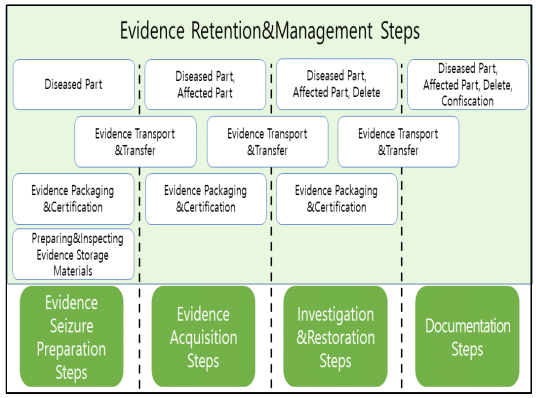

Fig. 4. Evidence Retention&Management Steps

역할을 수행하도록 구성하였다.

IV. 연구 검증

본 절에서 제안하는 모델을 표준 가이드라인과 비교 및 실제 대법원 판례에 적용하는 사례연구를 통해 제시한 모델의 타당성을 검증한다.

4.1 표준 가이드라인과의 비교

논문에서 제시한 모델의 세부 단계와 NIST의 'Guidelines on Mobile Device Forensics', TTA의 'Guidelines on Cellular Phone Forensics'와의 비교를 통해 본 모델에서 제시하는 절차를 검증하고자 한다. 절차를 Fig. 5.과 같이 도식화하여 비교한 결과 NIST와 TTA에서 제시한 단계들은 단계구성의 차이는 일부 존재하였으나, 모든 단계가 모델에서 제시하는 단계에 포함되는 결과를 확인할 수 있다.

또한, Table. 1.과 같이 모바일 포렌식 절차 모델과 다른 두 가지 절차 모델과 비교하여 동일한 절차 단계는 " O ", 유사한 절차 단계는 있지만 미흡한 경우는 " △ ", 절차가 존재하지 않는 경우는 " X "로 구분하여 서로 간에 매핑하여 분석된 조사표이다. 준비단계(△), 선별 및 보존단계(△), 검사 및 추출 단계(△), 증거 이송 및 이전(△)는 일부 절차에만 적용되고 새로운 데이터획득 단계(X)와 검토단계(X)는 미적용 된다.

준비단계는 NIST에는 해당하지 않으나, TTA에서 제시한 포렌식 도구 준비와 수사관의 훈련단계에 해당한다. 새로운 데이터획득 단계와 증거 검토단계

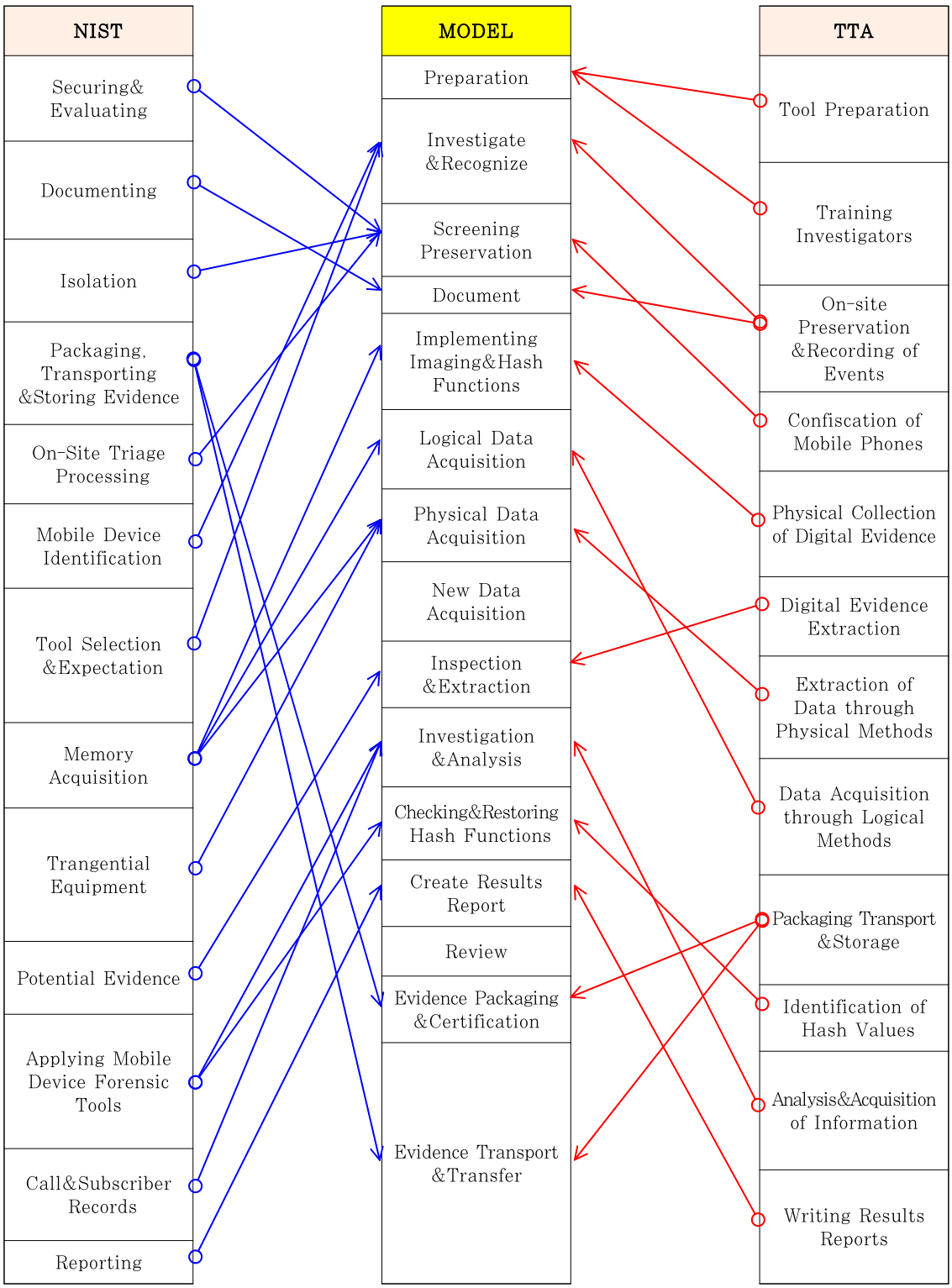

Fig. 5. Comparison with Other Model(Relative Procedure)

는 두 모델에서 제시하고 있지 않는 단계로 본 모델에서 최초로 제시하고 있는 단계이다.

NIST와 TTA에서는 증거 보존 및 관리를 한 가지 단계로 구성하고 있지만 본 모델에서는 증거 검토, 증거 포장 및 인증, 증거 호송 및 이전의 3단계로 세분화하여 구성하고 있으며, 특히 증거의 보존 및 관리의 측면에서 독립적인 단계로 구성하였다는 차이점을 보인다.

Table 1. Comparison with Other Model (Application)

Mobile Forensics Model for Improving Integrity		NIST	TTA
Evidence Seizure Preparation Steps	Preparation	X	O
	Investigate &Recognize	O	O
	Screening Preservation	O	△
	Document	O	O
Evidence Acquisition Steps	Implementing Imaging&Hash Functions	O	O
	Logical Data Acquisition	O	O
	Physical Data Acquisition	O	O
	New Data Acquisition	X	X
	Inspection& Extraction	O	△
Investigation &Restoration Steps	Investigation &Analysis	O	O
	Checking&Restoring Hash Functions	O	O
Documentation Steps	Create Results Report	O	O
Evidence Retention &Management Steps	Evidence Review	X	X
	Evidence Packaging &Certification	O	O
	Evidence Transport &Transfer	△	△

4.2 사례 연구(CASE STUDY)

사례 연구를 통하여 모델에서 제시한 신규단계의 적합성 검증을 실시하고자 한다. 연구 검증은 디지털 증거의 증거능력 인정요건을 구체적으로 언급하였던 대표적인 판례인 대법원 2007도7257 판결(일심회 사건)과 대법원 2013도2511(왕재산 사건)의 디지털 저장매체에 관련한 증거능력 인정요건과 증거 환부 이후 재 제출된 증거의 증거능력인정 여부를 판결한 대법원 2013도11233 판결을 중심으로 활용하고자 한다.

일심회 사건의 주요 판시사항은 디지털 저장매체로부터 출력한 문건의 증거능력이며, 왕재산 사건의 주요 판시사항은 정보저장매체에 기억된 문자정보 또는 그 출력물을 증거로 사용하기 위한 요건 및 정보저장매체 원본을 대신하여 저장매체에 저장된 자료를 '하드카피' 또는 '이미징'한 매체로부터 출력한 문건의 경우, 그 출력 문건과 정보저장매체에 저장된 자료가 동일하고 정보저장매체 원본이 문건 출력 시까지 변경되지 않았다는 점에 대한 증명 방법 및 '증거물인 서면'의 증거조사 방식이다. 두 판결 모두 법정에 제시한 증거(출력한 문건)가 당초 존재했던 원본으로부터 생성되었는지를 입증하는 것이 무결성을 보장하는 중요한 요건임을 설명하고 있으며, 차이점으로 일심회 사건에서는 전문법칙의 예외조건을 중심으로 판단하였다면 왕재산 사건에서는 무결성 입증과 예외 사항에 관해 논하였다.

일심회 사건은 무결성 보장을 디지털 저장매체 원본이 압수 시부터 문건 출력 시까지 변경되지 않았음을 증명하는 것으로 하고 있고, 왕재산 사건은 무결성 보장을 연계보관성(보관의 연속성 증명)과 연관됨을 의미하도록 하여 디지털 증거가 수사기관에 최초 압수되면서부터 법정에 제출되기까지 과정의 연계성에 주목하여 디지털 증거에 대한 압수·수색 이후 증거로 현출되기까지 일련의 절차에서 증거의 인위적 개작이 없었음을 증명한다면 이를 무결성이 보장됐음을 의미한다고 정의하였다. 두 사건은 모두 압수 당시 디지털 매체로부터 데이터를 복제하여 디지털 형태로 저장되어 있는 문서를 인쇄된 형태로 출력한 출력물을 증거물로 제출하였다는 공통점을 가지고 있다. 그렇다면 같은 증거물의 형태를 띠고 있는 두 가지 사건을 비교해본다면 무결성을 보장하기 위한 필요충분조건을 획득할 수 있을 것이다.

일심회 사건을 A라고 하고 왕재산 사건을 C라고 했을 때, 두 판결의 무결성 보장(B)을 Fig. 6.과 같

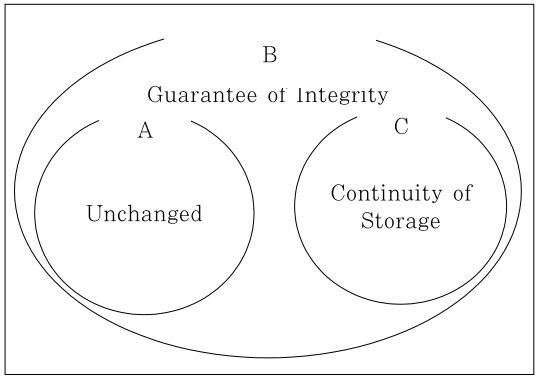

Fig. 6. A Comparative Case Study

이 정리할 수 있다.

무결성을 입증하는 방법으로 두 판결 모두 압수 매체에 대한 봉인, 녹화, 매체 이동과정, 해쉬값의 비교 등 종합적으로 사정을 고려하였으나, 왕재산 사건의 원심은 동일성과 필수불가결한 관계로 무결성(연계보관성)이 증명된다면 동일성 입증에 요구되는 방법으로 사용되는 해쉬값 비교 절차가 반드시 수반된다고 볼 수 없고 원본과 출력문건의 객관적인 검증결과 등 제반 조건을 종합하여 법관의 자유판단에 의하도록 하는 형사소송법 제308조의 자유심증주의를 준용하여 동일성 여부에 관하여 합리적으로 판단하도록 판시하였다.

이는 증거 보관 및 관리가 증거 압수 준비 단계부터 보고서 단계까지 포괄하는 별도의 단계로서 유지하는 것이 합당하다는 논리적 뒷받침의 자료로서 충분하다고 할 수 있다. 또한, 압수·수색 집행절차의 위법성과 증거능력 관련 내용으로 집행 시 적법여부와 압수·수색·검증영장의 장소 및 신체에 대한 압수수색의 과다여부를 따졌다.

증거가 위법하게 수집되었는지 과잉금지원칙을 적용하였는지를 확인하는 과정으로 증거가 적법하고 한정된 범위 내에서 수집되었는지가 중요한 요소이다. 과정 수행을 위해 사전에 포렌식 절차를 진행하기 위한 검증된 포렌식 도구의 준비, 수사관의 능력 배양과 증거수집 절차 및 계획 수립(사건의 개요, 압수수색검증 장소 및 대상, 정보저장매체 등의 유형과 규모 등) 등의 선행조건이 필요함을 의미한다.

선고 2013도11233 판결의 경우 주요 판시사항은 수사기관이 별개의 증거를 환부하고 후에 임의제출 받아 다시 압수한 경우, 제출에 임의성이 있다는 점에 관한 증명책임 소재와 증명 정도 및 임의로 제출된 것이라고 볼 수 없는 경우 증거능력을 인정할 수 있는지 여부이다.

본 대법원 판결에서는 수사기관에서 증거를 피압수자 등에게 환부한 후에 임의제출 받아 재 압수하였다면 증거를 압수한 최초의 절차 위반행위와 최종적인 증거수집 사이의 절차적 공백이 단절되었다고 평가할 수 있다고 인정하였으나 환부 후 다시 제출하는 과정에서의 강제적인 압수가 행하여지는 등의 수사기관의 우월적 지위를 활용할 수 있어 제출에 임의성이 있다는 점에 대해서 검사가 합당한 의심을 배제할만한 당위성을 증명하도록 하고 있고 임의로 제출된 것이라고 볼 수 없는 경우에는 그 증거능력을 인정할 수 없다고 판결요지를 언급하고 있다.

판결의 주요 쟁점은 위법수집증거 배제법칙 등에 관한 내용이지만, 본 대법원 판결에서 중요하게 살펴봐야할 점은 환부하고 후에 이를 임의제출 받아 다시 압수하였다면 그 증거를 압수한 절차의 적법성에 대한 증명 및 절차 위반행위와 최종적인 증거수집의 인과관계의 단절유무를 판단해야한다는 것이다.

디지털 증거의 특성상 데이터의 대량성과 변조의 용이성을 가지고 있어 방대한 데이터 중에 본 사건과 관련된 데이터만을 선별하고 불필요한 자료는 환부·삭제하는 절차를 거치게 된다. 환부·삭제된 자료의 복원 및 재수집은 법정에서 변조 여부 등 무결성에 대한 입증이 필요로 하고 입증이 불가능하다면 증거능력은 상실된다고 할 것이다.

4.3 무결성 향상을 위한 모바일 포렌식 모델 정리

디지털 증거는 법의학에서 활용하고 있는 일반 증거들에 비해 전자적 특성을 띠고 있어 증거능력을 입증하기 위한 검증된 방법을 사용하여야한다. 일반적으로는 압수가 된 전체 데이터의 해쉬값을 비교하여 그 원본성 및 무결성을 입증하였다. 하지만 증거의 증명력을 보장하기 위해서는 단순한 해쉬값의 비교로만은 입증하기 어려우며, 증거의 증명력 확보는 증거보존 및 관리단계, 증거 분석 및 복원단계, 보고서 작성단계를 준수하여야 발현될 수 있다. 증명력 확보는 법적 절차의 준수와 함께 무결성 보장에 있다. 증거의 무결성을 보장하기 위해서는 대다수의 수사관 및 분석관이 사용하기 위한 모델의 제시가 필요하며, 제시된 모델은 법·제도적으로 무결성을 입증하도록 원칙을 준수하여 모바일 기기에 부합하게 적용될 필요가 있다. 또한, 기술의 변천사에 맞게 새로운 기기

가 출시될 때마다 보안기술 수준도 높아지게 되어 이러한 특성에 맞게 획득 방법이 새로이 추가될 경우가 많기에 변화의 반영이 필수적이다. 앞서 제시한 모바일 포렌식 모델은 다음과 같은 사항을 반영하여 무결성을 보장받을 수 있도록 절차를 구성하였다.

본 연구의 한계로 새로운 데이터 획득단계를 모델의 절차에 반영하였지만 새로운 데이터 획득 기법은 기술의 성숙도와 기기별 특성을 고려한 분류 및 검증이 필요한 부분으로 향후 연구에서 심도 있게 다루고자한다.

V. 결론 및 향후연구

본 연구에서는 모바일 포렌식과 관련된 선행연구와 NIST 및 TTA의 표준 가이드라인에서 제시하는 절차의 핵심요소를 추출하여 5가지 단계와 15개의 세부항목을 도출하였으며, 단계별 절차 수행의 명확한 분리를 통해 무결성을 보장받을 수 있는 모바일 포렌식 모델을 제시하였다.

포렌식 단계 구성 시 디지털 증거의 일반원칙과 법·제도적 절차에 위배되지 않도록 증거의 증명력을 보장하기 위한 증거 보관 및 관리 단계의 별도 구성, 새로운 데이터 획득 단계, 증거 검토단계 등 모바일 기기의 발전과 개인 정보보호 인식의 성숙도가 반영된 차별화 단계를 포함하여 높은 신뢰성과 진정성을 바탕으로 모바일 포렌식 수행이 가능할 것이다.

따라서 본 연구에서 제시한 모바일 포렌식 모델의 일반화를 통해 신뢰할 수 있는 분석이 이루어졌다면, 법관의 심증형성에 기여 할 수 있으므로 수사기관의 증거능력 확보 및 활용도 측면에서 큰 도움이 될 것으로 기대한다.

본 연구의 향후 연구목표는 다음과 같다.

첫째, 제시한 모델의 현장 적용 가능성 검증을 위해 포렌식 전문가를 대상으로 설문조사를 실시하고 그 결과를 바탕으로 실증적인 타당성을 검증하는 것이다. 이를 위해 최신 대법원 판례를 사례화하여 모델 전반의 유용성에 대한 지속적인 검증 노력이 필요할 것이다.

둘째, 신규 기술을 적용한 모바일 기기에 맞는 새로운 데이터 획득 기법 적용의 필요성을 도출하고 분류 및 부분적 선별을 통해 실험환경을 구성하여 모델에서 제시한 절차를 수행하여 무결성 보장 여부를 검증한다.

마지막으로 본 연구에서 제시한 모델의 타당성과 유용성이 검증된다면 본 모델을 활용하여 디지털 증거능력 수준 평가항목을 도출하고 수준 측정 평가표를 제시함으로서 디지털 증거능력 수준 측정이 가능하게 하여 디지털 증거의 무결성 및 신뢰성에 관한 사법기관의 판단기준을 마련하고자 한다.

References

[1] Thomas P, Owen P and McPhee D, "An Analysis of the Digital Forensic Examination of Mobile Phone", 2010 Fourth International Conference on Next Generation Mobile Applications, Service and Technologies, pp. 25-29 Jul. 2010

[2] Goel A, Tyagi A and Agarwal A, "Smartphone Forensic Investigation Process Model", International Journal of Computer Science&Security (IJCSS), Vol. 6, no. 5, 322-341, Oct. 2012

[3] Willassen S, "Forensics and the GSM mobile telephone system", International Journal of Digital Evidence, Vol. 2, no. 1, pp. 1-17, Spring. 2003

[4] Sang-su Jo, Yong-tae Shin, "An Improvement on Integrity Assurance Processes for Digital Evidence", Journal of The Korean Institute of Information Scientists and Engineers 39(2), pp. 184-191, Apr. 2012

[5] Rick Ayers, Rick, Sam Brothers, and Wayne Jansen, "Guidelines on Mobile Device Forensics", NIST Special Publication 800-101 Revision 1, May. 2014

[6] Yang-sub Kwon, "A Study on the Evidence capability of Digital Evidence form cases", Korea Institute of Information Security&Cryptology, 26(5), pp. 44-53, Oct. 2016

[7] Myung-sun No, "Digital Forensics Theory", Korean Society of Forensics,

Mediabook, Dec. 2018
[8] TTA, "Guidelines on Cellular Phone Forensics", TTAS.KO-12.0059, Dec. 2007
[9] Doo-won Jeong, "Digital Forensics Framework Based on Digital Evidence", Department of Information Security Graduate School Korea University, Dec. 2018
[10] Kwang-yul Lee, Choi Younsung, Haelahng Choi, Seungjoo Kim, Dong-ho Won, "Digital Forensics Procedure for Current Evidence Laws", Journal of The Korea Institute of Information Security & Cryptology, 18(3), pp. 81-91, Jun. 2008
[11] Dong-hyoun Shin, "A study of digital evidence seizure methods with regard to human rights", Joural of Digital Forensics 11(8), pp.69-84, Jan. 2014.
[12] Emilio Raymond Mumba, H.S. Venter, "Mobile Forensics using the Harmonised Digital Forensic Investigation Process", 2014 Information Security for South Africa (ISSA), IEEE, 1-10, Aug. 2014.
[13] Soo-woong Eo, Wooyeon Jo, Seokjun Lee, Taeshik Shon, "Ensuring the Admissibility of Mobile Forensic Evidence in Digital Investigation", Journal of The Korea Institute of Information Security & Cryptology, 26(1), pp. 135-152, Feb. 2016.
[14] Byong-sun Kwack, "A study on Problems and improvements of digital forensic investigation", Korean Law Association Law Review, 42, pp. 171-191, May. 2011.
[15] Jae-bong Kim, "Admissibility of Digital Evidence and Identification", Hanyang Journal of Law, 31(1), pp. 171-195, 2014.
[16] Dong-guk Kim, Seong-Young Jang, Won-Young Lee, Yong-Ho Kim, Chang-hyun Park, "An Effective Control Method for Improving Integrity of Mobile Phone Forensics", Journal of the Korean Society for Information Protection, 19(5), Oct. 2009.

〈저자소개〉

김 영 준 (Young-june Kim) 정회원
2015년 2월: 한국교통대학교 항공운항학과 졸업
2019년 2월: 국민대학교 보안법무학과 석사
2019년 3월~현재: 아주대학교 국방디지털융합학과 박사과정
〈관심분야〉 디지털 포렌식, 데이터 복원, 사이버전, 정보보호

김 완 주 (Wan-ju Kim) 종신회원
1998년 2월: 서울과학기술대학교 전자공학 학사
2008년 1월: 국방대학교 전산정보 석사
2017년 2월: 아주대학교 NCW공학 박사
2017년 3월~현재: 아주대학교 국방디지털융합학과 겸임교수
〈관심분야〉 사이버전, 국방전술통신, 정보보증, 사이버위험예축

임 재 성 (Jae-sung Lim) 종신회원
1983년 2월: 아주대학교 전자공학 학사
1985년 2월: KAIST 영상통신 석사
1994년 8월: KAIST 전자공학 박사
1998년 3월~현재: 아주대학교 소프트웨어융합학과 교수
〈관심분야〉 Military&Mobile Communications, Wireless Networks, 사이버전