情報保護學會論文誌
第19卷 第5號, 2009. 10

모바일 포렌식의 무결성 보장을 위한 효과적인 통제방법

김 동 국,[1†] 장 성 용,[2‡] 이 원 영,[2] 김 용 호,[3] 박 창 현[4]
[1]에이쓰리시큐리티, [2]국립 서울산업대학교, [3]경기대학교, [4](주)유넷정보통신

An Effective Control Method for Improving Integrity of Mobile Phone Forensics

DongGuk Kim,[1†] SeongYong Jang,[2‡] WonYoung Lee,[2]
YongHo Kim,[3] Changhyun Park[4]
[1]A3 Security, [2]Seoul National University of Technology,
[3]Kyonggi University, [4]Unet Co., Ltd.

요 약

포렌식 수사 절차상의 무결성을 입증하기 위한 방안으로 해쉬 함수 알고리즘을 적용한 디지털 증거의 경우, 무결성이 손상되면 그 자료는 폐기되어야만 했다. 즉, 주요 사건의 핵심 부분에 대한 증거 확보를 위해서는 삭제 영역에 대한 증거 복원이 필수적임에도 불구하고, 전체적인 해쉬값이 처음 해쉬값과 달라 증거 데이터가 훼손됨으로 인하여 결정적인 증거 능력 확보에 어려움이 있었다. 본 논문에서는 이와 같은 문제점을 해결하기 위한 방안으로서 새로운 모바일 포렌식 절차 모델인『Evidence-Finder (이하 E-Finder) 모바일 포렌식 절차 모델』을 제안한다. E-Finder 절차는 5개 영역의 총 15개 절차 모델로 구성되며 E-Finder 절차를 기존 NIST(National Institute of Standards and Technology)모델, Tata Elxsi Security Group 모델과 비교 및 고찰하였다.

이로 인하여, 현재까지 모바일 포렌식 분야에서 표준화 되지 않고, 검증되지 않은 방법론을 개선하는 기대효과를 달성하였다.

ABSTRACT

To prove the integrity of digital evidence on the investigation procedure, the data which is using the MD 5(Message Digest 5) hash-function algorithm has to be discarded, if the integrity was damaged on the investigation.

Even though a proof restoration of the deleted area is essential for securing the proof regarding a main phase of a case, it was difficult to secure the decisive evidence because of the damaged evidence data due to the difference between the overall hash value and the first value.

From this viewpoint, this paper proposes the novel model for the mobile forensic procedure, named as 『E-Finder(Evidence Finder)』, to solve the existing problem. The E-Finder has 5 main phases and 15 procedures. We compared E-Finder with NIST(National Institute of Standards and Technology) and Tata Elxsi Security Group. This paper thus achieved the development and standardization of the investigation methodology for the mobile forensics.

Keywords: Mobile Forensic, Control Method, NIST, JTAG

접수일(2009년 6월 16일), 게재확정일(2009년 8월 23일)

† 주저자, share21@a3sc.co.kr
‡ 교신저자, syjang@snut.ac.kr

I. 서 론

1.1 연구 필요성 및 목적

정보의 매개체 및 문명의 이기로 사용되는 이동통신 기술이 급속하게 발전됨에 따라 이를 악용한 범죄의 증가 및 범죄 기술은 갈수록 증가되고 있다. 따라서 모바일 이동매체관련 범죄의 대응 기술을 통한 모바일 포렌식의 무결성 확보방안은 함께 발전되어야 할 분야로 대두되고 있으며, 수사현장에서 확보된 휴대폰의 데이터가 변조되지 않고 향후 재판에 중요한 증거로써 채택이 될 수 있도록 하는 통제 방안 절차는 중요한 요소로 부각되고 있다.

특히, 주요 사건의 핵심 부분에 대한 증거 확보를 위해서는 삭제 영역에 대한 증거 복원이 필수적임에도 불구하고,[1] 증거 취득시 적용된 해쉬값과 달라 증거 데이터에 대한 무결성이 훼손됨으로서 그 증거자료는 폐기해야만 했다. 하지만 주요 사건의 핵심이 되는 삭제영역에 대한 무결성이 보장된다고 판명되면 증거 데이터로서의 활용을 고려할 수 있게 되었다.

따라서 본 연구의 목적은 보다 효율적인 무결성 보장 방안을 수립하기 위해서 다양한 휴대폰 기종에 범용적인 적용이 가능한 기술적인 대안으로 삭제영역의 무결성 보장을 통한 증거능력을 확보하여, 향후 휴대폰의 디지털 증거가 사건 현장에서 수집된 이후 법정에 제출될 때까지 신뢰성 확보를 위한 무결성을 보장하는 데 있다. 이와 같은 효과적인 무결성 보장을 위해서 획득, 분석, 복구 절차 단계에서의 절차연속성(Chain of Custody)과 법적인 증거능력, 증명력을 확보할 수 있는 기술기반의 증거 처리 및 수사절차인 15단계 통제 절차를 제안한다. 이는 향후 수사 환경에 새로운 기술적 모바일 포렌식 절차 모델을 적용함으로서 보다 효율적인 현장 연구에 기여하는데 있다.

1.2 연구 범위 및 방법

본 논문의 연구 범위로는 국내 CDMA 방식의 휴대폰을 중심으로 멀티미디어 기능을 제공하고 있는 퀄컴사의 Baseband Chip인 MSM(Mobile State Modem) 6500을 위주로 적용하였다. MSM6500의 모델 선정으로, 동영상을 지원하는 휴대폰의 트렌드에 부합하고 시중에서 범용적으로 폭넓은 인기가 있는 휴대폰을 테스트 기기로 사용 및 검토하여, 통제 절차를 수립하는 방법을 연구하였다. 여기에는 휴대폰을 연결하는 전자장비 및 디지털 증거물 수집·장비도 포함된다.

이와 같이 휴대폰을 활용, 모바일 포렌식에 추가적인 절차를 도입하여 정립하기 위해서 획득, 분석 및 복원 과정에 이르는 모바일 포렌식의 기술요소를 파악하는 것을 연구 과제로 선정한다. 이를 위해서 첫째, [2]Serial(UART) 통신 방식의 물리적인 데이터 획득 방식을 대상으로 선정한다. 현재 국내에서는 물리적으로 데이터를 획득하는 방식이 JTAG 방식[3]인데, 이 방식은 제조사가 양산시 JTAG 포트를 오픈하지 않는 휴대폰 모델도 있어 데이터 획득이 어려우므로 새로운 물리적인 데이터 획득 방식을 구성한다.

둘째, 모바일 포렌식의 기술요소를 통제 절차에 적용했을 때 무결성을 보장하기 위한 대안으로 새로운 기술요소를 정립한다. 일반적으로 데이터의 무결성은 최초 데이터 획득 시 원본에 대한 사본 이미지를 생성하여 해쉬 함수 적용 후 나중에 복원 단계에서 원본 데이터의 해쉬값과 동일한지 비교하여 확인한다. 본 연구에서 E-Finder 통제절차 경우 사용자 파일시스템(Embedded File System)을 분석하여 전화번호 등이 기록 보관된 일반영역과 파손된 삭제영역으로 구분하고 2단계 해쉬 함수를 적용한 후 해쉬값 16진수(128바이트)가 달라졌는지 확인하는 무결성 점검 절차를 구성한다.

셋째, 새로운 기술요소를 모바일 포렌식의 절차상에 추가하여 적용하기 위해 미국 NIST의 '휴대폰 분석에 관한 가이드라인'[4], Tata Elxsi Security

1) 시스템 포렌식에서는 디스크의 물리적인 손상이 있을 경우, 손상되지 않는 영역의 분리 복구가 불가능하였으나, 모바일 포렌식에서는 손상되지 않는 영역의 분리 복구가 가능하다[12].

2) UART(Universal Asynchronous Receiver/Transmitter) 방식 : 휴대폰 내부의 Serial 통신 포트(UART) 제어 명령어를 이용한 접근 방식으로 데이터를 전송하기 위한 송수신 프로토콜인 Async HDLC를 이용 물리적인 방법으로 플래시 메모리의 바이너리 데이터를 Dump하여 데이터를 획득하는 방식

3) JTAG 방식은 JTAG 디버거 등을 이용한 플래시 메모리 데이터 수집으로서 단말기 내부의 플래시 메모리 영역 전체를 단말기 프로세스와 연계된 내부 명령어를 이용하여 Dump하는 물리적인 획득 방식

4) [NIST SP 800-101] 2007 Guidelines on Cell Phone Forensics [16] NIST(National Institute of Standards and Technology)는 미국상무부 기술관리국 산하의 각종 표준과 관련된 기술을 담당하는 연구소로서 산업현장에서 절대적으로 필요로 하는 각종 기술과 측정 분야에 국가 기준이 되는 표준을 선정하고 개발, 적용하는 업무를 담당하고 있다. NIST Publications는

Group의 '윈도우 모바일 포렌식 절차'를 비교·검토한 후 새로 적용될 절차상의 필요한 요소를 추가하고 효과적인 통체 절차를 구현하여 신뢰성을 증대시킨다.

연구 방법을 살펴보면, 1장에서는 모바일 포렌식에 관련된 연구의 필요성 및 목적과 연구 범위 및 방법에 대하여 기술한다. 2장에서는 모바일 포렌식의 이론적 고찰로서 기존 모바일 포렌식에 관한 문헌 연구 동향을 조사·분석하여 기존 연구의 한계점 및 필요성에 대한 새로운 연구 방향을 제시하고 개념에 대하여 살펴본다. 3장 및 4장에서는 기존 디지털 포렌식 절차 모델인 NIST, Tata Elxsi Security Group의 윈도우 모델과의 비교를 통한 새로운 E-Finder 절차 단계를 수립하여 장·단점을 기술하고 새로운 15단계의 통제 절차 단계에 대해 연구한다. 5장에서는 E-Finder 절차 모델의 15단계가 휴대폰 증거획득에서 보고서 단계까지 현실적으로 적용되는지를 검증하기 위하여 가상의 사례연구(Case Study)를 통해 제안해보고 NIST 절차 모델과 비교하여 기술한다. 6장은 결론 및 향후 연구 과제로서, 유럽기반의 GSM방식의 증거데이터획득을 위한 절차 기법에 관한 연구를 향후 연구 과제로 정하며, 점차 글로벌화 되어가는 국내 환경에 적용이 가능한 이동통신 방식의 무결성을 보장하는 방법에 관한 연구를 제시한다.

II. 모바일 포렌식의 문헌 연구 및 정의

2.1 모바일 포렌식의 문헌 연구

모바일 포렌식 관련 연구들은 국내외 컴퓨터 포렌식을 모바일 디바이스에 맞게 적용된 것이라 할 수 있다. 모바일 디바이스는 디지털 컨버젼스를 맞이하여 매우 빠른 속도로 진화되고 있으며 국내외 포렌식 관련 연구도 디지털 포렌식에 관련된 연구가 주류를 이룬다.

먼저 수사 절차 및 무결성 확보를 위한 연구로 Anup Ramabhadran[12]는 모바일 기기의 특성과 휘발성 및 비휘발성에 관하여 절차 단계마다 구체적인 차폐장치, 이미징, 해쉬 함수를 적용하는 절차 단계가 공통적으로 적용되어 있고 삭제 영역의 무결성을 검증하는 단계는 존재하지 않으므로 데이터 무결성을 확보하는데 어려움이 발생할 수 있다고 하였다.

홍성경[11]은 디지털 증거의 신뢰성에 대하여 문제를 제기할 경우 이를 방어하기 위하여 기존의 포렌식 절차모델을 기반으로 디지털 증거의 무결성 확보를 위한 새로운 디지털 포렌식 절차 모델을 제안하였다. 새로운 절차 모델은 5가지 모델을 비교하여 공통적으로 적용되는 필수 절차 단계로 『준비단계』, 『조사단계』, 『분석단계』, 『보고서 단계』인 4단계를 필수 절차로 삼아 디지털 포렌식 실무 적용 방안을 수립하였지만, 모바일 포렌식에서 필요한 JTAG 방식을 보완한 Serial(UART) 통신 포트를 이용하는 접근 방식으로 구현하기에는 한계가 있다. 임동환[8]은 기존의 경찰청 디지털 증거처리 표준 가이드라인을 분석하여 살펴보고 디지털 증거 수사 절차와 일반 범죄의 증거 수집 절차를 비교한 다음, 이원화 된 절차를 통합하여 새로운 통합형 표준 절차 프로세스 모델을 제안하였다. 특히, 인트라넷 기반 환경에서 압수·수색 절차 및 물리적 증거와 디지털 증거의 상호연관성을 염두에 두고 수사실무 적용방안을 제시하였다. 하지만, 새로운 통합된 디지털 포렌식의 절차 모델을 모바일 포렌식 관점에서 구현하는 데는 어려움이 따른다. 그리고 김기환[1]은 휴대폰에서 디지털 증거가 저장되는 플래시 메모리의 저장구조를 통하여 디지털 증거를 획득하는 방안과 별도로 해쉬 함수를 이용한 디지털 증거의 무결성 입증방안을 고찰하였다. 하지만, 모바일 포렌식 관점에서는 복원 단계에서 디지털 증거가 훼손되더라도 EFS2(Embedded File System2)의 삭제 영역에 대한 무결성을 입증하여 법정에서 형사절차상 증거 능력을 인정받기 위한 증거 능력 확보 방안이 필요하다.

그리고 기술적인 측면에서 살펴보면, Svein Y.Willassen[17]은 삭제영역을 복구하기 위하여 JTAG 방식과 메모리를 PCB판에서 분리하고 BGA 리페어 방식을 이용하여 물리적으로 데이터를 획득하는 기술을 제시하고 있다. 성진원[3]은 국내 휴대폰의 CDMA방식에 따른 기술 및 데이터 획득에서의 문제점, 획득한 데이터 분석에서의 문제점을 분석하고 대안을 모색하였다. 그리고 이경민[4]은 퀄컴의 QPST를 사용하여 휴대폰 개발 도구를 이용해 CDMA 휴대폰에 적용하여 데이터 획득, 분석의 가능성을 제시하였다. 또한, 김용호[2]는 복구된 디지털 데이터에 대한 원인 규명과 대상에 대한 분석이 가능하도록 하기 위해 정형화된 분석 기법과 모델을 개발하였다.

마지막으로, 법적인 대안으로는 이광열[6] 등이 국

FIPS(Fedeal Information Processing Standard :컴퓨터 보안에 관련된 미연방정부 정보처리 표준)를 준용하여 미연방정부의 컴퓨터 보안이나 호환성에 대한 필요성에 의해 NIST에서 만드는 표준 및 지침을 정의함.

내 현행 증거법을 분석하고 경찰청의 '디지털 증거처리 표준 가이드라인'을 따라 각 절차와 관련되어진 증거법칙을 관련 단계에 적용하여, 디지털 포렌식 절차의 궁극적인 목적인 디지털 증거의 사용을 위해서 현행 증거법상의 증거능력과 증명력을 기준으로 포렌식 절차를 분석하였다. 또한, 탁희성[10]은 디지털 증거의 정의와 디지털 증거를 압수수색할 때의 유의점및 적법한 범위 및 절차에 대한 발표를 하였고, 오기두[7]는 컴퓨터 범죄를 정의하고 그 유형에 대해 조사하여, 우리나라의 현재 법 규정과 해외 선진국 여러 나라의 법 규정에 관해 연구조사 및 압수수색의 범위 및 관련성을 위주로 나열하였다. 위 연구 논문들에서의 주된 측면은 무결하게 증거자료를 취득하는 방법과 디지털 증거의 증거능력에 대한 외국사례 및 법령을 예로 설명하여, 어떻게 수집하고, 복원 및 처리해야 증거능력을 얻을 수 있고, 또 어떤 경우에 증거능력이 상실될 수 있는지에 대한 연구 결과라 할 수 있다.

이와 같은 기존의 연구방향을 통하여 디지털 포렌식 절차모델에 관한 비교를 통한 새로운 절차 모델의 제시와, 발전되는 모바일 포렌식 기술개발에 따르는 무결성을 확보하는 추가 절차에 관한 연구가 필요하였으며, 절차 모델을 기반으로 하는 방법 및 구체적인 통제항목의 연구가 역시 필요하게 되었다. 또한, 수사 절차마다 모바일 포렌식의 절차 단계별 증거법칙의 근거기준도 마련되어야 한다. 따라서 연결성의 원칙을 중심으로 현재까지의 모바일 포렌식 절차를 신기술 개발에 따른 무결성 보장 방안에 관한 방법으로 제안한다.

수사절차 단계별 무결성에 관한 효과적인 방법을 개발하기 위해, 모바일 포렌식의 기술적인 관점에서 새롭게 고려해야 할 기술 요소인 단말기 접속 형태에 따른 플래시 메모리 데이터 수집에 관한 기술 요소, 단말기 내부의 플래시 메모리에 대한 구조 분석, A 이동통신사의 파일 포맷 Property분석 및 복원에 관하여 연구한다.

그리고 모의 수사 절차 시나리오에 E-Finder 절차방법을 기존 모바일 포렌식 절차 모델과 비교하여 효과적인 측면에서 적용 및 검증한다.

2.2 모바일 포렌식의 정의

포렌식은 컴퓨터 보안영역 및 법 학회에서 컴퓨터 증거를 수집하기 위한 필요성으로 등장하였으며 1984년 초 FBI 과학수사연구소와 법 집행기관에서 컴퓨터 기기를 압수수색하는 문제와 압수된 기기로 잠재적 증거를 발견하는 것에 중점을 두고 연구되기 시작하였다[15]. 이러한 연구 방향은 인터넷과 정보통신 기기의 발전으로 인하여 1998년부터 새로운 미디어매체나 출력물로부터의 디지털 증거(Digital Evidence)자체에 관심을 갖게 되었으며 그 명칭 또한 디지털 포렌식으로 사용하게 된 것이다.

이러한 디지털 포렌식은 "정보처리기기 등 디지털 소스로부터 각종 행위에 대한 사실관계를 확정하거나 증명하기 위해 필요한 디지털 증거를 보존, 수집, 증명, 식별, 분석, 해석, 기록, 제출을 하기 위하여 과학적으로 이끌어내고 증명하는 방법" 이라고 정의할 수 있으며 디지털 포렌식 기술은 "컴퓨터 등 디지털기기를 매개로 이루어지는 행위에 대한 법적인 증거자료를 확보하기 위하여 컴퓨터 시스템과 네트워크 등 디지털 소스로부터 정보를 수집, 분석 및 보존절차를 통하여 법적 증거물로서 제출할 수 있도록 하는 일련의 행위"로 정의할 수 있다[14].

디지털 포렌식은 적용 대상 및 주요기술 분야에 따라 [표 1]과 같은 유형으로 구분되어진다[5,9]. 모바일 포렌식은 미국, 영국과 같이 모바일 포렌식의 연구가 활성화된 국가의 경우 내장저장장치가 컴퓨터의 저장장치와 같은 포맷인 MP3, PMP, 카메라와 내장저장장치가 다른 포맷인 PDA 및 네비게이터 포렌식으로 구분되어진다. 그 중에서도 개인 휴대통신장비인 휴대폰은 빠르게 휴대폰을 이용한 범죄의 발생 확률은 높다고 할 수 있다. 따라서 모바일 포렌식은 기존의 데이터 저장장치와는 다른 파일 시스템을 가지는 휴대가 가능한 컴퓨터나 정보처리 장치를 사용하여 이루어지는 모든 사실관계를 확정 또는 증명하기 위해 증거

[표 1] 디지털 포렌식의 유형

유형	정의
시스템 포렌식	포렌식에서 많이 연구된 분야로서 하드디스크, CD, USB 메모리 등 비휘발성 저장장치로부터 증거물을 획득하고 분석하는 것을 말한다.
네트워크 포렌식	네트워크를 통하여 전송되는 데이터를 수집하거나 트래픽과 로그를 분석하여 증거로 활용하는 분야이다. 라우터나 기타 네트워크 장비들에 남아 있는 로그를 분석하여 침해여부를 분석한다.
모바일 포렌식	모바일 포렌식은 PDA, 전자수첩, 휴대폰, MP3 등 휴대용 기기에 저장된 내용을 증거로 확보하는 기술이다.
포렌식 어카운팅	기업의 분식회계, 탈세 등 각종 부정을 조사할 때 기업의 ERP나 전산회계의 데이터베이스를 분석하는 분야이다. 일반적으로 SAP/R3나 오라클ERP 등 ERP기반 회계시스템으로 나눌 수 있다.

를 수집, 식별, 획득, 보존, 문서화하여 법정에 제출하는 일련의 행위라고 정의하고 있다[4].

III. E-Finder 모바일 포렌식 절차 방법

3.1 새로운 모바일 포렌식 절차 방법의 필요성

기술적인 데이터 획득 방법을 통한 데이터의 증거능력에 대해서는 법원에서 신뢰할 수 있도록 무결성 방안이 보장되어야 하므로, 디지털 증거의 경우 쉽게 조작이 가능하다는 취약성으로 전문법칙을 적용하는 것이 타당하다. 현재 모바일 포렌식의 적용 범주인 휴대폰의 경우도 실제 직접 진술이 아닌 다른 형태의 간접 보고이므로 전문법칙의 예외에 해당이 됨으로서 증거능력으로 인정받을 수 있다. 국내 경우 형사소송법(제313조) 제1항에 보면 진술서의 경우 진술에 의한 성립의 진정함이 증명되어야 하나, 디지털 증거의 경우에는 진술자의 의미를 원진술자가 아닌 포렌식 전문가 성립의 인정을 통해 증거 능력을 인정할 수 있다는 것으로 해석하는 것도 고려할 수 있다[6]. 이와 같은 디지털 속성에 따라 증거 데이터는 0 또는 1의 특성으로 인하여 1의 비트가 틀려지더라도 데이터의 무결성이 위배되므로 수개월 동안 수사관이 작업한 증거 데이터도 해쉬값이 틀려진다면 증거 데이터를 폐기처분할 수밖에 없었다. 하지만 새로운 메모리 페이지 맵 스트럭처 분석기법을 통하여 플래시 메모리에 사용자 영역인 일반 영역과 삭제 영역을 구분하고 삭제 영역이 손상이 되지 않는 것이 입증이 된다면 증거능력으로서 활용할 수 있는 길이 열리게 되었다.

또한 기존 데이터 분석 방식은 시스템 포렌식 관점의 파일 시스템 단위(EX. 섹터 등)로 분석하는 데이터 무결성 검증방안이 존재한다. 해쉬 함수의 경우에는[5] 인위적인 분류 방식의 적용 이후에 데이터 분류 후 가능하다.

하지만, 본 논문에서는 휴대폰 접속 당시의 증거데이터를 소규모의 단위 및 영역별로 분석 및 조회 할 수 있게 되었다. 휴대폰 전체의 메모리 구조 분석 알고리즘을 통해, 필요한 영역의 증거 데이터만 분석하는 무결성 검증 방법의 적용이 가능하게 되었다. 즉, 현재까지의 데이터 무결성 보장을 위한 해쉬 적용 등의 방식과 다른 점은 휴대폰 접속 순간 부터 메모리 영역 스캔 및 구조 분석 과정을 통하여 좀 더 신속하고, 안전한 무결성 검증 방법 적용이 가능한 점이 다르다.

이와 같이 본 논문에서는 어려운 수사현실을 위한 데이터 획득, 분석 및 복원에 이르기까지 새로운 절차의 필요성을 절감하였고, 기존의 모바일 포렌식 절차 모델과 비교 분석하여 새로운 15단계의 절차 모델을 수립하였다.

3.2 E-Finder 절차 모델과 기존 절차와의 비교 고찰

본 논문에서 제시하는 E-Finder절차모델은 휘발성 증거수집과 비휘발성 증거수집으로 나눠지며, NIST와 Tata Elxsi Security Group 모델 및 E-Finder 모바일 포렌식 절차 모델을 비교하여 새로운 기술에 적용되는 단계 절차를 추가함으로써 데이터 무결성이 향상되는 부분을 고려해 보았다.

[표 2]처럼 NIST는[6] 총 4단계인 보존, 수집, 검사와 분석, 보고서 작성인 4단계로 구분되는 반면, [4] E-Finder 절차 모델은 『현장 보존 단계』, 『데이터 획득(논리적, 물리적) 단계』, 『검사 및 추출 단계』, 『증거데이터 분석 단계』, 『결과보고서 단계』인 6단계로 구분하는 절차를 고려하였다. 이 단계 외에 NIST에서 고려되고 있지 않은 부분인『이미징을 통한 해쉬 함수 절차 단계』, 『E-F 물리적인 데이터 획득 단계』, 『2차 해쉬 함수 구현 및 복원 단계』, 『증거 관리 단계』는 새로운 데이터 추출도구의 개발에 따라 절차의 개발 및 무결성 보장을 위한 향상을 위해 필요한 것으로 고려되었다.

지금까지 E-Finder와 NIST 모델을 비교하였으며 본 논문에서 제안되는 E-Finder의 제안 모델의 장점을 살펴보면 다음과 같다.

첫째, 기술 기반으로 활용도가 높다. 휴대폰의 새로운 기능 추가에 따라 데이터 획득을 위한 새로운 절차

5) 시스템 포렌식은 파일시스템 섹터 단위의 정해진 논리적인 영역에 데이터가 존재하므로 비인가자에 의한 데이터의 위·변조가 가능하지만 모바일 포렌식은 플래쉬 메모리의 물리적인 파일시스템으로써 블락 단위의 영역에 구성되어 휴대폰 접속 시점에서 구조적인 알고리즘에 따른 비정형화된 영역에 로그 파일이 저장된다. 또한, 물리적인 증거 데이터의 저장 위치인 메모리맵 분석에 어려움이 따르므로 위·변조가 불가능하다

6) NIST에서 제안한 휴대폰 포렌식 절차는 4단계로서 1) 보존은 범죄현장의 디지털 증거의 보존, 포장, 이송과 보관 2) 수집은 디지털 증거물에 대한 수집 3) 검사와 분석은 최대한 증거물을 훼손시키지 않으면서 증거물 분석 4) 보고서 작성은 분석결과에 대한 보고서 작성으로 구분된다[4].

〔표 2〕 E-Finder 모바일포렌식 절차 모델 비교

X : 존재 하지 않음

단계	E-Finder 절차 모델	Elxsi Security Group	NIST
1	사전 준비 단계	사전 예비	X
2	이미징 및 1차 해쉬 함수 구현단계	X	X
3	차폐 관리 단계	통신 차단	X
4	현장 보존 단계	보존	보존 현장 확인 기록
5	조사 및 인식 단계	조사 및 인식	
6	문서화 단계	현장 기록	
7	논리적인 데이터 획득 단계	휘발성 증거수집	수집
8	물리적인 데이터 획득 단계	비휘발성 증거수집	수집
9	E-F 물리적인 데이터 획득 단계	X	X
10	검사 및 추출 단계	보관 및 이송	보관 및 이송 차폐 관리
11	증거 보관 및 이송 단계	검사	검사
12	조사 및 분석 단계	분석 복원 이미징 1차 해쉬	분석 및 복원
13	2차 해쉬 함수 구현 및 복원 단계	X	X
14	결과 보고서 단계	보고서	보고서
15	보존 및 증거 관리 단계	리뷰	X

기법의 하나인 Serial(UART) 통신 기법으로 MSM 6500이상 모델에서도 S/W구현 방식으로 물리적인 데이터 획득이 가능하게 되었다.

둘째, 증거 능력의 향상을 가져왔다. 플래시 메모리의 EFS2영역에서 일반영역과 삭제 영역을 구분하여 비록 전체 증거 데이터 중 일부분의 무결성이 훼손 되었더라도 주요 증거 확보 영역인 삭제 영역의 무결성이 보장됨으로서 증거 능력의 향상을 가져왔다.

셋째, 보편적이면서 실무적인 측면에서 데이터의 무결성 향상을 가져왔다. 기존 절차 방식에서는 『차폐 관리 단계』또는 『이미징 및 1차 해쉬 함수 구현단계』들이 없었지만 E-Finder 절차 모델에서는 차폐장치를 현장 수사 시 보유하고 있지 않을 경우를 대비하여 미리 이미징 작업을 수행 후 해쉬 함수를 구현하는 단계

〔표 3〕 모바일 포렌식 15단계 절차모델 단계

E-Finder	정의
사전준비 단계	휴대폰 데이터 수집 및 분석을 위한 제반사항으로 모바일 포렌식 도구에 대한 준비 및 조사관에 대한 교육이 이루어져야 한다.
이미징 및 1차 해쉬 함수 구현단계	차폐장치를 보유하지 않은 현장에서는 빠른 시간 내에 데이터 이미징 작업을 거쳐 원본 데이터와 같이 사본 데이터에도 해쉬 함수를 적용하여 원본 파일과 동일시함을 증명해야 한다.
차폐관리 단계	증거수집에 앞서서 휴대폰의 전자적인 장치인 통신을 차단한다
현장보존 단계	비인가자의 침입으로부터 범죄 현장을 보존하고 증거물의 훼손을 방지한다.
조사 및 인식단계	최초현장 보존단계부터 수사관은 적절하게 조사계획을 세우고 잠재적인 증거물을 확보한 후 현장을 평가한다.
문서화 단계	수사현장을 사진으로 스케치하거나 범죄현장을 문서로서 모든 디지털 증거와 물리적인 증거를 정확하게 기술한다.
논리적인 데이터 획득 단계	메모리로부터 휘발성 증거를 획득한다. 만약 배터리가 없다면 메모리에 보존되어 있는 증거 데이터가 소실될 위험이 존재한다. · USB Sync 방식의 모바일 포렌식 툴을 이용한 휴대폰 데이터의 획득 · 파일전송 프로토콜을 이용한 데이터 획득 · 제조사의 PC 소프트웨어를 통한 데이터 획득
물리적인 데이터 획득 단계	모든 데이터를 Bit 단위로 Dump한 데이터를 획득한다. · 직접메모리 접근방식, JTAG디버거 장비를 이용한 데이터 획득 · BCG기반의 리볼링 방식을 이용한 데이터 획득
E-F 물리적인 데이터 획득 단계	휴대폰마다 다른 입력신호의 사용과 CPU의 차이 및 JTAG 핀의 비표준화에 따른 단점을 보완한 새로운 물리적인 데이터를 획득한다. · 인터페이스 멀티박스 장비인 JTAG 디버거를 통한 데이터 획득 · Serial(UART)방식의 데이터 획득
검사 및 추출 단계	수사관은 수집된 증거 데이터를 검사하여 사건의 핵심이 되는 데이터를 추출하고 선별한다.
증거보관 및 이송 단계	패킹, 수송, 저장단계로써 수집된 저장 데이터가 변질되거나 파괴되는 것을 막고 증거물을 보관하며 이송할 때에는 절차연속성을 유지해야 한다.
증거데이터 분석 단계	플래시 메모리의 EFS2를 조사하고 분석하여 일반 영역, 삭제 영역, 비활성 영역을 구분하여 분석한다.
2차해쉬 함수 구현 및 복원 단계	· 삭제된 영역과 일반영역을 구분한 2단계 해쉬 함수를 적용하며 주요 증거로 채택되는 삭제영역의 무결성이 보장이 된다면 비록 다른 영역이 훼손 되더라도 증거로 채택되어 활용이 가능해야 한다. · 사용자가 확인할 수 있는 Phone File System으로 재구성하여 통신사별 Property규칙을 적용하여 증거 데이터를 복원한다.
결과 보고서단계	작성자는 결과 보고서에 작성내용에 대해 책임을 진다는 원칙을 서술하고 서명한다.
보존 및 증거관리 단계	증거보관실의 운영을 위한 조건과 증거자료관리 및 준수사항에 대해 기술한다.

를 우선적으로 부여함으로써 통신으로 인한 데이터 훼손을 미연에 방지할 수 있다.

따라서 본 연구에서는 〔표 3〕과 같이 새로운 모바일 포렌식의 기술적인 요소를 적용한 총 15단계의 절차 모델 단계를 제시한다.

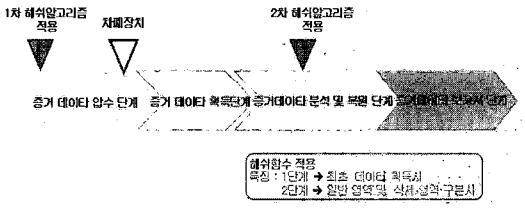
E-Finder 모바일 포렌식 15단계 절차 모델에서 차별화되는 가장 중요한 단계는 13단계인 『2차 해쉬함수 구현 및 복원단계』이다. 이 단계에서는 플래쉬 삭제 영역과 일반 영역을 구분하고 다시 한 번 해쉬 함수를 이용하여 데이터 무결성의 이상 유무를 확인하는 절차가 필요하다. 이렇듯 번거롭게 해쉬 함수의 이상 유무를 다시 한 번 점검하는 절차는 절차 연계성의 원칙에 위배되지 않으면서 데이터의 삭제 영역에 대한 무결성이 보장이 된다면 비록 데이터의 일부분이 훼손되더라도 삭제 영역의 증거복원 능력에 따라 법적 증거로서 활용가치가 있다는 시사점을 가질 수 있다. 즉, 기존에는 사본 이미지를 전체 이미지화하여 해쉬 함수를 적용한 반면에, 삭제 영역의 훼손 여부만을 가려냄으로써 증거능력으로 인정받을 수 있는지를 고려하게 되었다. 기존 절차에 의한 데이터의 훼손여부에 따라 삭제되어 처리하지 못한 미해결 사건이나 미제출로 인한 해결 불가능한 사건들도 이 새로운 절차를 적용하면 증거로서의 활용가능성을 높일 수 있게 된다. 이는 기존 모바일 포렌식 절차 모델과 비교를 통한 증거 절차를 구체적으로 제시한 단계로서 이와 같은 모델 절차를 활용함에 따라 법원에서는 새로운 증거 데이터로서의 가치를 가질 수가 있다.

또한 단계절차가 세분화됨에 따라 해당되는 절차에 적절한 방법과 새로운 기술적인 대응방법을 가질 수가 있다. 『E-F 물리적인 데이터 획득 단계』의 JTAG방식은 접속방식에 따른 상이한 신호체계로부터 발생하는 데이터 획득의 어려움을 보완하는 단계이다. 즉, 소프트웨어 구현만으로 물리적인 데이터를 획득하는 UART 방식으로서 새로운 데이터의 무결성을 보장하는 효과적인 절차로 활용될 수 있다. 이와 같이 새로운 모바일 포렌식 모델 절차를 단계별로 수행을 하면 효과적인 데이터 무결성 보장이 가능하다.

IV. E-Finder 모바일 포렌식 절차 15 단계

4.1 모바일 포렌식 절차 방법 단계

모바일 포렌식 무결성 보장을 위한 효과적인 E-Finder 통제 방법은 모바일 포렌식의 증거물 압수, 증거물 획득, 증거물 분석 및 복원, 보고서 단계의 일련의 과정을 포괄하며 단계별 세부 계획은 하위 모듈에서 상세하게 정의된다.



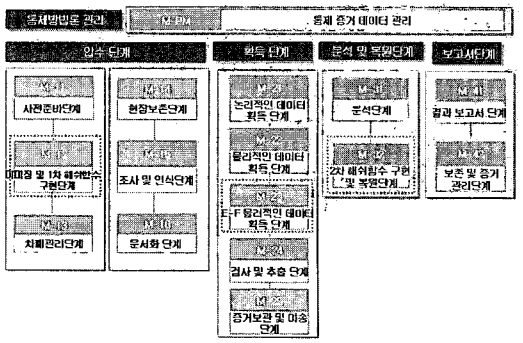
〔그림 1〕 통제 방법의 단계별 정의

〔그림 1〕에 보면 데이터의 무결성 보장을 위하여 해쉬 함수 적용을 2단계에 걸쳐 적용함으로써 보고서를 제출하기 전에 증거물이 훼손 되지 않았음을 보장할 수 있어야 하는 절차 연속성 원칙을 준용한다.

모바일 포렌식의 통제 방법의 구성도인 〔그림 2〕를 살펴보면 총 5개의 영역에서 총 15개의 절차 모델로 구성되어 있다. 통제 프로세스 매니지먼트 단계에서는 통제 프로세스의 모든 단계에서 사용되는 절차와 기법을 서술하여 각 단계마다 절차연속성 원칙과 법적인 기준을 적용하여 무결성 보장을 위한 프로세스에 대한 수준과 가치를 확보한다.

증거물 압수 단계는 수사현장에서 조사자의 휴대폰과 관련되어지는 증거의 확보 및 모바일 포렌식 도구의 장비점검 필요 항목으로서 총 6단계인『사전준비단계』,『이미징 및 1차 해쉬 함수 구현단계』,『차폐관리단계』,『현장보존단계』,『조사 및 인식단계』,『문서화 단계』로 구성된다.

『증거물 획득단계』는 증거유형을 논리적, 물리적, E-Finder 물리적(UART)증거로 구분하여, 사건의 핵심이 되는 데이터를 획득하고 선별하는 단계로서 총 5단계인『논리적인 데이터 획득단계』,『물리적인 데이



〔그림 2〕 E-Finder 통제 방법의 구성도

터 획득단계』, 『E-Finder 물리적인 데이터 획득단계』, 『검사 및 추출단계』, 『증거보관 및 이송단계』로 구성된다.

『증거물 분석 및 복원 단계』는 전체 파일 시스템 중 EFS2 를 사용자 영역과 삭제 영역으로 구분하고 삭제 영역의 무결성이 보장되면 증거능력을 확보할 수 있는 단계로서 총 2단계인 『증거데이터 분석단계』, 『2차 해쉬 함수 구현 및 복원단계』로 구성된다.

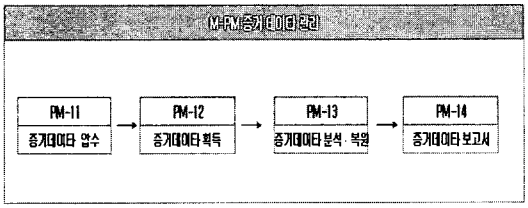
『증거물 보고서 단계』는 사건에 대한 정보, 증거물에 대한 정보 등을 명확하고 객관성 있게 6하 원칙에 따라 작성하고 보관하는 단계로 총 2단계인 『결과 보고서 단계』, 『보존 및 증거 관리 단계』로 구성된다.

4.1.1 증거데이터 관리 단계

증거데이터 별로 관련 증거법칙인 증거의 신뢰성, 위법 수집 증거 배제법칙, 전문법칙의 예외, 증명력을 다룸으로써 무결성의 기준을 수립하여 절차 연속성 원칙을 유지하여야 한다.

증거데이터 관리 단계의 흐름도는 〔그림 3〕에 따라 총 4단계의 절차로 이루어진다.

증거 데이터 관리 단계는 절차연속성을 확보해야 하며 각 단계마다 법적인 기준을 따르는 가치를 확보해야 한다. 〔표 4〕는 증거 데이터 관리 단계별 관련 법적 기준을 정리한 것이다.



〔그림 3〕 증거 데이터 관리 흐름도

〔표 4〕 증거 데이터별 관련 법적 기준

증거 데이터 관리	관련 법적 기준
증거 데이터 압수 단계	· 증명력 기준
증거 데이터 획득 단계	· 전문법칙의 예외
증거 데이터 분석 및 복원 단계	· 증명력 · 증거의 신뢰성 · 위법수집 증거법칙
증거 데이터 보고서 단계	· 증명력

4.1.2 증거 데이터 압수 단계

(1) 증거 데이터 압수 개요

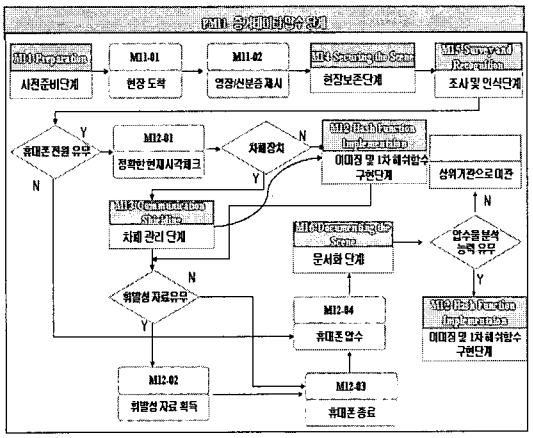
『증거데이터 압수』단계에서는 증거데이터의 수행에 있어 수사현장에서 조사자의 휴대폰 외 관련되어지는 증거의 확보와 분석을 위한 도구의 구비 및 장비점검을 통한 신속한 수사가 이루어지도록 해야 한다. 더불어 범죄현장을 문서화하고 증거 수집에 앞서 휴대폰의 전자적인 장치인 통신을 차단한다.

(2) 증거 데이터 압수 흐름도

『증거데이터 압수』흐름도는 〔그림 4〕처럼 각각의 흐름도에 따르는 화면에 관한 통제항목으로 구성되어진다.

증거 데이터 압수 단계에서 가장 중요한 요소는 고가의 차폐장치 보유 유무에 따라 흐름도가 차이가 난다. 즉, 차폐장치를 현장에 보유하고 있을 경우 정상적인 흐름도를 따라 수행하지만 없는 경우에는 외부로부터 전자파 및 통신으로부터 데이터의 무결성을 보호하고자 처음 상태의 휴대폰으로부터 데이터의 이미지 복제를 통한 해쉬 함수를 적용한다.

차폐장치가 없는 경우 이미지 백업을 할 시간적 여유가 없더라도 휴대폰은 물리적인 메모리 접근 방식으로 휴대폰 접속 순간 이미 휴대폰은 물리적으로 슬립 상태에 놓이게 된다. 이것은 차폐장치를 적용했을 때처럼 통신 등의 기능을 차단하는 것이다. 이런 이후에 메모리에 접근하여 영역별로 구조 분석이 가능하기 때문에 원천적인 데이터 무결성 검증 방법 적용이 가능하며 실제 재 구동 이후에 내부 로그 영역에 남게 된다. 따라서 휴대폰 내부 데이터를 분석하는 알고리즘



〔그림 4〕 증거데이터 압수 흐름도

〔표 5〕 증거 데이터 압수 세부 통제 항목

세부 통제 항목	PM11-압수 단계 상황 정리
· M11-01 현장 도착	현장 도착
· M11-02 영장/신분증제시	휴대폰 수거에 어려움이 예상되는 경우 미리 영장 및 수사기관의 신분증을 통하여 제시
· M14 현장 보존 단계	압수물과 사용자 분리, 전원 확보, 현장 스케치
· M15-1 조사 및 인식단계	압수 대상 휴대폰 상태파악(파손 유무) 하여 사진을 찍어 증거데이터 확보
· 차폐장치 여부 확인	차폐장치가 없는 경우에는 M12 복제 및 1차 해쉬 함수 구현단계를 수행하고 차폐장치가 있는 경우에는 M12-01과 같이 정확한 현재시간을 확인 후 휘발성 자료유무에 따라 자료 획득 함
· M13 차폐 관리 단계	휴대폰 전원 상태 유무 확인하기 전 전자파 차단 장치를 통하여 무결성 상태 확인
· M12-01 정확한 현재시각	휴대폰시간과 현재 시간을 비교하여 현재 시간을 정확하게 기록
· M12-02 휘발성 자료획득	휘발성 자료 유무를 확인하여 휘발성 자료를 획득
· M12-03 휴대폰 종료	휘발성 자료 유무를 확인하여 휴대폰을 종료
· M12-04 휴대폰 압수	휴대폰을 압수 시 조사자에게 대체 휴대폰을 제공
· M16-01 문서화 단계	사건 개요 및 확보된 증거데이터 내용 상세하게 작성
· M12-이미징 및 1차 해쉬 함수 구현단계	차폐장치가 있는 경우에 문서화 단계 이후 휴대폰의 데이터 획득 단계 수행

을 통하여, 로그 데이터 및 관련 사항 분석을 통한유효성 검증이 가능 하다.

다음은 차폐장치를 보유했을 때의 정상적인 수행과정이다. 수사관은 현장에 도착 시 미리 신분증과 영장을 통해) 현장을 보존하여 협의자의 휴대폰을 압수하고 수사관이 제공하는 대체 휴대폰을 사용하며, SMS와 같은 문자 등이 수신이 되는 경우를 대비하여 차폐장치를 통해 통신을 차단한다. 휴대폰이 정상인 경우는 휘발성 자료를 획득하고 확보된 데이터 외에 증거물에 대하여 내용을 상세하게 작성해야 한다.

〔표 5〕는 증거 데이터 분석 및 복원 단계 세부 통제 항목을 정리한 사항이다.

4.1.3 증거 데이터 획득 단계

(1) 증거 데이터 획득 단계 개요

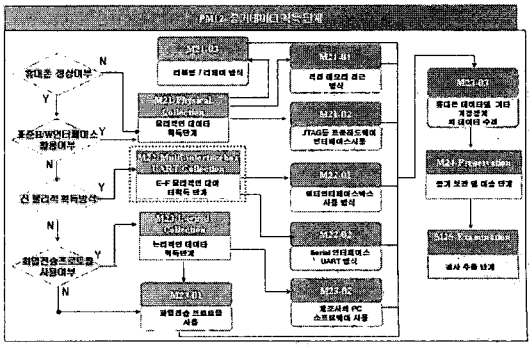
『증거 데이터 획득』단계에서는 증거의 획득 유형을 논리적 물리적으로 구분하고 새로운 모바일 포렌식 도구를 이용하여 증거 데이터를 획득한다. 획득한 증거 데이터는 향후 사건의 핵심이 되는 데이터로서 선별되어진다.

(2) 증거 데이터 획득 단계 흐름도

『증거데이터 획득』흐름도는 〔그림 5〕의 흐름도로 나타나며 〔표 6〕에서처럼 각각의 흐름도에 따르는 화면에 관한 통제항목으로 구성되어 진다.

먼저 물리적인 데이터 수집방법으로 1) 휴대폰이 파손된 경우에는 기판에서 메모리를 떼어내어 메모리 리더기를 통하여 수집하는 방법, 2) 기판 훼손 시 리볼링 방법으로 클론폰을 제작하거나 리페어 방법으로 메모리 소켓을 이용하는 방식, 3) 휴대폰이 정상작동 시 표준 하드웨어 인터페이스 방식인 JTAG을 통하여 CPU에 직접 명령을 전송하여 메모리를 전송하는 방식이 있다. 하지만 이와 같은 방식은 휴대폰사의 JTAG 핀맵인 칩셋이 달라서 신호체계가 다르기 때문에 모든 휴대폰에서 데이터를 획득하는데 어려움이 따른다. 따라서 이와 같은 단점을 보완하고자 새로운 Serial 인터페이스인 UART 방식과 다양한 휴대폰의 신호체계를 스캔하여 표준 신호체계로 변환해주는 멀티인터페이스 방식을 제안한다.

다음은 논리적인 데이터 수집 방식으로써 파일전송 프로토콜의 경우 파일 시스템의 파티션처럼 논리적인 공간에 저장되어 있는 것을 파일 전송명령을 주어 해당 파일을 PC로 다운받는 것으로서 A 휴대폰의 PC-매니저가 해당된다. 둘 째, 휴대폰의 플래쉬 메모리를 설계하는 퀄컴사의 QPST라는 프로그램을 PC에 설치하여 플래시 메모리의 정보를 획득할 수 있다. 이와 같이 데이터를 물리적인 방식과 논리적인 방식으로 획득할 경우 획득한 전체 데이터에 대하여 제일 먼저 복



〔그림 5〕 증거 데이터 획득 흐름도

〔표 6〕 증거 데이터 획득 세부 통제 항목

세부통제 항목	PM12-획득 단계 상황 정리
· M21-01 직접 메모리 접근방식	휴대폰이 정상이 아닌 경우 기판에서 메모리를 직접 메모리에 연결하여 증거 데이터를 획득하는 방식과 휴대폰 외부 저장장치인 메모리 카드를 미디어 리더기를 사용해 SD와 같은 플래시 메모리카드의 데이터를 획득하는 방식이 있다.
· M21-02 JTAG등 표준하드웨어 인터페이스 사용 방식	JTAG와 같은 표준 하드웨어 인터페이스 방식을 사용하여 물리적인 데이터를 획득한다. · 기판에서 JTAG 포트확인 · TDI, TDO, TCK등의 JTAG연결 포트에 케이블링 · MSM 칩, 플래시 메모리 등의 정보 확인 · 플래시 메모리 덤프
· M21-03 리볼링/리페어 접근방식	휴대폰의 기판이 훼손이 된 경우에는 기판에서 메모리를 떼어내고 리볼링 및 리페어하여 클론폰을 제작하는 데이터 획득 방식과 메모리 소켓을 이용한 데이터 획득방식이 있다.
· M22-01 멀티인터페이스박스 사용 방식	JTAG의 단점을 보존하는 방식으로, 상이한 신호체계를 표준화된 신호체계로 변환해주는 Firmware 방식의 멀티인터페이스 방식이다. · 기판에서 JTAG 포트확인이 불가능할 시 TTA포트를 통하여 멀티 인터페이스박스로 접속하는 방식 · MSM 칩, 플래시 메모리 등의 정보 확인 · 플래시 메모리 덤프
· M22-02 Serial(UART)통신 사용 방식	Serial 인터페이스(UART)방식의 모바일 포렌식 툴을 이용한 물리적 데이터 획득 방식이다. · USB to Serial 포트 어댑터(젠더)를 통하여 TTA 포트로 접속 · MSM 칩, 플래시 메모리 등의 정보확인 · 플래시 메모리 덤프
· M23-01 파일전송 프로토콜 사용	논리적인 공간에 저장되어 있는 것을 파일 전송명령을 주어 PC로 파일을 다운받는 방식이다.
· M23-02 제조사의 PC 소프트웨어 사용	휴대폰 제조사는 퀄컴사에서 제공하는 QPST와 같은 프로그램을 PC에 설치하여 플래시 메모리의 정보를 획득하는 방식이다.
· M23-03 휴대폰 데이터 및 기타 저장장치의 데이터 수집	휴대폰 데이터 및 기타 저장장치의 데이터를 수집한다.
· M24 Preservation 증거보관 및 이송 단계	패킹, 수송, 저장 단계로써 획득한 저장 데이터가 변질되거나 파괴되는 것을 막는다.
· M25 Examination 검사추출 단계	수사관은 수집된 증거데이터를 검사하여 사건의 핵심이 되는 데이터를 획득하고 선별한다.

제를 한 후 복제한 사본으로 1단계 해쉬 함수를 적용하여 원본과 동일함을 보장해야 한다.

마지막으로 휴대폰 외에 기타 저장장치의 데이터를 수집한 다음 『증거보관 및 이송단계』에서는 패킹, 수송, 저장단계에 수집된 데이터가 변질되거나 파괴되는 것을 막아야 한다. 『검사추출 단계』에서는 증거 데이터를 조사하기 전에 처음 획득한 원본 데이터를 보호하고 복제된 증거 데이터를 검사하여 핵심이 되는 데이터를 추출하고 선별해야 한다.

〔표 6〕은 증거 데이터 획득 세부 통제 항목을 정리한 사항이다.

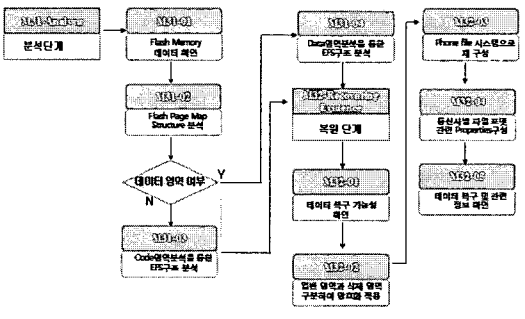
4.1.4 증거 데이터 분석 및 복원 단계

(1) 증거 데이터 분석 및 복원 개요

플래시 메모리의 전체 파일 시스템 구조분석을 통해 코드 영역과 데이터 영역으로 구분하고 데이터 영역은 일반 영역과 삭제 영역으로 분리한다. 일반 영역은 다시 폰파일시스템으로[7] 재구성 한 다음 2단계 해쉬 함수를 적용하여(일반영역과 삭제영역에 별도의 MD5 해쉬 함수 적용) 수사 절차 단계과정에서 증거 데이터의 변동여부를 확인한다.

(2) 증거 데이터 분석 및 복원 단계흐름도

『증거데이터 분석 및 복원 단계』에서는 〔그림 6〕과 같이 플래시 메모리의 데이터는 물리적인 파일시스템 구조 분석을 통해 코드 영역과 데이터 영역을 확인하여 전체 파일 시스템 구조 분석을 한다. 『증거데이터 복원 단계』에서는 삭제 데이터의 복구 가능성 유무를 확인 한다. 복구 가능성이 확인이 된 일반 영역 과 삭제 영역은 다시 폰파일 시스템으로 재구성한 후 2단계



〔그림 6〕 증거 데이터 분석 및 복원 단계 흐름도

7) 유저화일시스템으로써 sms, phone book, image file, movie file, memo, etc 등이 해당된다.

〔표 7〕 증거 데이터 분석 및 복원 단계 세부 통제 항목

세부 통제 항목	PM12-획득 단계 상황 정리
· M31-01 플래시 메모리 데이터 확인	조사관이 살펴야 할 휴대폰 내 정보 확인 - 전자메일, MMS, 사진, 동영상, 전화번호 등
· M31-02 플래시 페이지 맵 스트럭쳐 분석	EFS의 전체적인 페이지 스트럭쳐 분석
· M31-03 데이터영역분석을 통한 EFS 구조 분석	EFS구조 중 데이터 영역 분석
· M32-01 Data 복구 가능성 확인	삭제 영역에 대한 복구 가능성을 확인
· M32-02 일반 영역과 삭제영역을 구분하여 암호화 적용	각각 일반 영역과 삭제 영역을 구분하여 2단계 해쉬 함수를 적용하여 법원에 제출하기 위한 최종적인 증거데이터의 무결성 훼손 여부를 확인
· M32-03 폰파일시스템으로 재구성	일반 영역 및 삭제 영역을 사용자가 확인할 수 있는 시스템을 재구성
· M32-04 통신사별 파일 포맷 관련 Properties 구성	통신사 별 파일 Property 규칙을 적용하여 복원을 위한 조사 구성을 함
· M32-05 데이터 복구 및 관련 정보 확인	사용자가 읽을 수 있는 파일 포맷인 SMS, Phone Book, Image, 동영상등으로 복원

암호화 알고리즘을 적용하여(일반영역과 삭제영역에 별도의 MD5 해쉬 함수 적용) 서로 간에 무결성이 위배되었는지 확인한다.

재구성되어진 파일들은 통신사별로 Property[8]를 구성한 후 사용자가 읽을 수 있는 파일 포맷인 SMS, Phone Book, Image, 동영상 등으로 복원한다.

〔표 7〕은 증거 데이터 분석 및 복원 단계 세부 통제 항목을 정리한 사항이다.

4.1.5 증거 데이터 보고서 단계

(1) 증거 데이터 보고서 개요

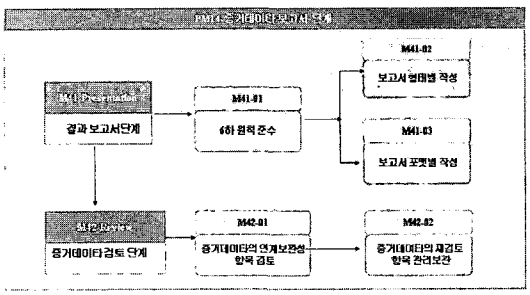
사건에 대한 정보, 증거데이터에 대한 정보, 분석에 대한 정보, 세부적인 분석 결과, 보고서 결과는 명확하고 객관성을 갖도록 6하 원칙에 따라 작성되어야 한다.

8) A 폰파일포맷 분석 알고리즘, B 폰파일포맷 분석 알고리즘 등 각 통신사별 파일포맷 분석 알고리즘으로 정의된다.

(2) 증거 데이터 보고서 단계 흐름도

『증거데이터 결과 보고서 단계』는 모든 모바일 포렌식 절차상에 일어난 사항들을 정리하는 과정이며 사건의 유무죄를 판단하는 결과에 해당되는 과정이다. 보고서는 〔그림 7〕과 같이 사건에 대한 정보, 증거데이터에 대한 정보, 분석에 대한 정보, 첨부 자료, 세부적인 분석 결과 및 보고서 결과는 명확하고 객관성 있게 6하 원칙에 따라 작성되어야 한다. 보고서는 웹 브라우저 형태의 GUI 작성, PDF 포맷별 파일 보고서, txt, rtf, doc, hwp등 여러 가지 포맷을 따라 작성되어야 한다.

『증거 데이터 검토 단계』에서는 증거 데이터의 입출력에 대한 절차연속성 항목을 검토해야 하며 차후 수사 및 재판 과정에서 재검증이 필요할 경우를 대비하여 제조사, 제조연도 등의 항목을 검토해야 한다. 〔표 8〕는 증거 데이터 보고서 단계 세부 통제 항목을 정리한 사항이다.



〔그림 7〕 증거 데이터 보고서 단계 흐름도

〔표 8〕 증거 데이터 보고서 단계

세부 통제 항목	PM12-획득 단계 상황 정리
· M41-01 6하 원칙을 준수	언제, 어디서나, 누가, 무엇을, 어떻게, 하였는지의 관점에서 내용을 기술
· M41-02 보고서 형태별 작성	텍스트 형태나 GUI 형태별로 작성
· M41-03 보고서 포맷별 작성	사용자가 요구하는 형태의 포맷별 작성 - HTML 또는 PDF 별로 작성 등
· M42-01 증거 데이터의 절차연속성 항목을 검토	증거 데이터의 입출력 과정에서 데이터의 무결성을 보장하기 위한 절차연속성 항목을 검토
· M42-02 증거 데이터의 재검토 항목 관리 보관	차후 수사 및 재판 과정에서 재검증이 필요할 경우를 대비하여 제조사, 제조연도 등의 항목을 검토

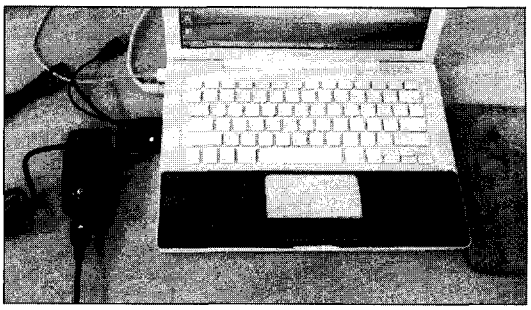
V. 모바일 포렌식 절차의 가상 시나리오

5.1 사례 연구를 통한 검증

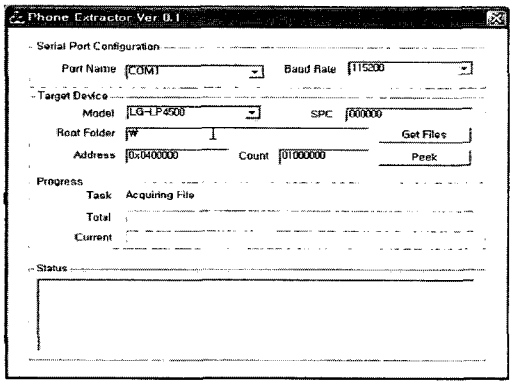
본 논문에서 제안되는 시나리오는 실무적으로 수사의 무결성을 검증하는 효과적인 방법이다. 국내 휴대폰의 경우 고객의 취향에 따라 생명주기가 짧아지고 휴대폰 기술이 발전됨에 따라 모바일 포렌식 수사 절차의 새로운 적용이 필요하게 되었다. 따라서 지금까지 시도되지 않는 새로운 E-Finder의 15가지 통제 절차 중 3가지 주요 차별화 단계인 『M22-Multi InterfaceBox & UART 절차 단계』, 『M32-02 일반영역과 삭제영역에 해쉬 함수 적용 단계』, 『M32-04 통신사별 파일 포맷관련 Property구성 단계』를 기존의 NIST 절차모델과의 비교를 통하여 고찰 한다.

사례 연구를 통한 검증 방법의 시나리오 단계는 다음과 같다.

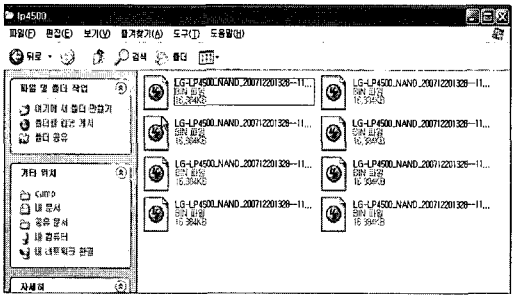
〔압수 · 획득 단계〕
2008년 11월 OO사무실에서 사건 당시 수사 현장에서 도착한 조사관은 『사전 준비 단계』에 따라 현장 스케치 및 증거 수집 장비 현황을 살펴보았다. 수사관은 차폐장치가 없는 것을 발견하고 증거 데이터의 무결성을 위하여 『이미징 및 1차 해쉬 함수 구현단계』를 구현하였다. 수사관은 외부로부터 현장 보존을 위하여 『현장 보존단계』절차에 따라 범죄 현장을 파악하고 모든 증거를 문서로서 언제, 누가, 어떻게 했는지 등을 문서로서 남기기 위한『현장보존단계』, 『조사 및 인식 단계』를 구현 하였다.
조사자로부터 압수한 휴대폰 A사-LP4500은 외관상으로는 이상이 없지만 어떠한 정상 작동도 되지 않았다. 조사관은 휴대폰을 정밀 분석해보니 조사자의 의도적인 행위로 인하여 휴대폰 내부 메모리 영역에 대한 물리적인 손상이 있는 것으로 확인이 되었고 JTAG 핀맵인 포트 확인이 불가 하여, 종류 별로 JTAG 포트의 신호 체계에 따른 모든 휴대폰의 데이터를 획득하는데 어려움이 발생하였다. 따라서 『E-F 물리적인 데이터 획득 단계』인 Serial (UART)통신 포트 기반의 Phone Extractor 도구[12]를 활용하여 〔그림 8〕과 같이 휴대폰을 Phone Extractor 도구와 접속하여 〔그림 9〕와 같이 정보를 입력하고 〔그림 10〕처럼 A사-LP4500의 바이너리 데이터의 물리적인 획득이 가능하게 되었다. 또한 획득된 데이터는 『증거 보관 및 이송 단계』, 『검사추출 단계』에 따라 증거 데이터가 변질되거나 파괴되는 것을 방지하고 수사관은 획득된 증거 데이터를 검사하여 핵심이 되는 데이터를 획득하고 선별하였다.



〔그림 8〕 Phone Extractor 접속[12]



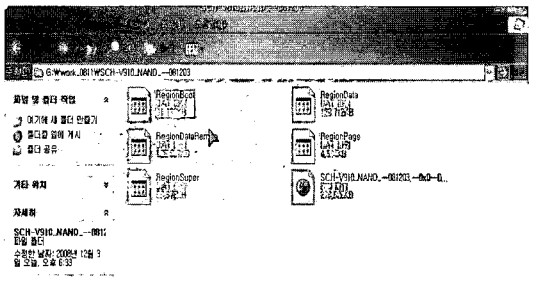
〔그림 9〕 Phone Extractor 도구



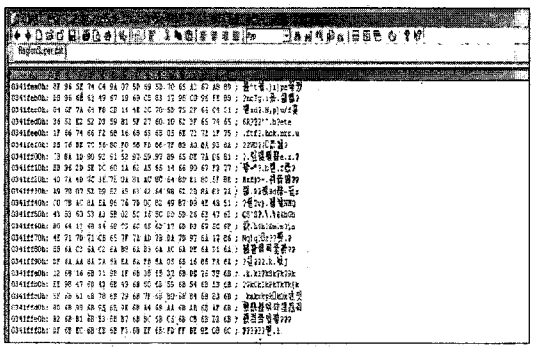
〔그림 10〕 Serial(UART) 통신방식의 데이터 획득

〔분석 · 복원 단계〕
휴대폰은 플래시 메모리의 모든 데이터를 플래시 메모리 구조분석인 『M31-02 Flash Page Map Structure 분석』을 통해 EFS2(Embedded File System2)와 디바이스 드라이버, 메모리 맵등을 분석 하였다. 그리고 〔그림 11〕처럼 영역 별로 구조화 되어진 데이터별로 구분 한 후 물리적으로 손상되지 않은 플래시 메모리 영역을 『M32-02 일반영역과 삭제 영역을 구분하여 암호화 적용』단계를 통하여 휴대폰의 일반 영역과 삭제 영역 중 〔그림 12〕과 같은 삭제 영역에 관한 구조적인 분석을 하

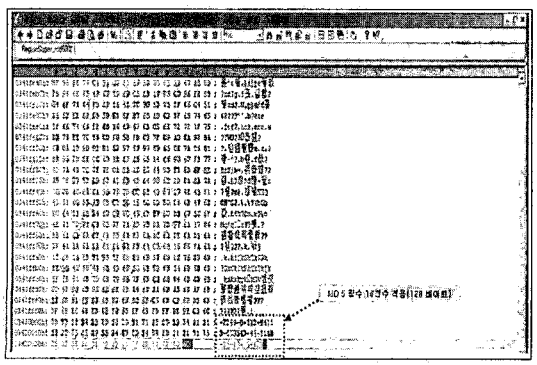
였다. 구조적인 분석 결과, 전체 이미지 중 삭제 영역의 데이터에 해쉬 함수의 키 값을 확인한 결과, 훼손 되지 않았음을 확인 할 수 있었다. 즉, 수사관은 주요 증거 데이터가 시스템 포렌식에서는 디스크의 물리적인 손상이 있을 경우 폐기처분이 될 수 있는 상황이 예상되었지만 주요 증거 데이터인 [그림 13]과 같이 전체 이미지 중 삭제 영역의 데이터에 대한 무결성 검증으로, 수사관은 비록 증거 데이터가 일부 훼손이 되었지만 주요 증거인 삭제 영역에서 데이터의 증거 능력을 갖출 수가 있었다.



[그림 11] 영역별 덤프 데이터



[그림 12] 삭제 영역

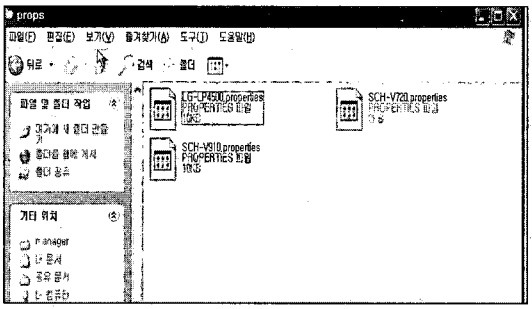


[그림 13] MD5 해쉬 함수 적용 후 삭제 영역

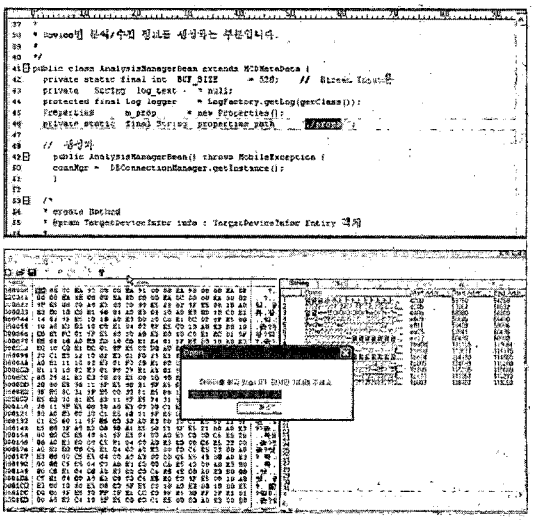
[복원 · 보고서 단계]

삭제 데이터 영역으로 구분되어진 증거 데이터는 『M32-03 Phone File 시스템으로 재구성』단계를 통하여, [그림 14], [그림 15]과 같이 『M32-04 통신사별 파일 포맷 관련 Property 구성』단계에서 A사의 Property의 규칙을 적용하여 구성한다. 구성되어진 해당 Property를 적용하여 분석 프로그램을 실행한 후 『M32-05 데이터 복구 관련 정보 확인』단계를 통하여 [그림 16], [그림 17]의 SMS, 사진 정보, 전화번호등 사용자 파일 포맷으로 복원하였다.

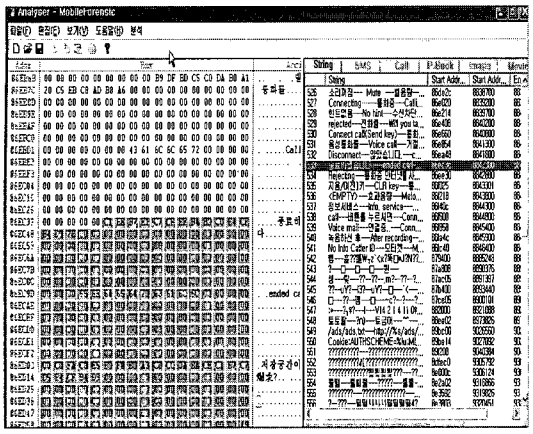
증거 데이터는 사건에 대한 정보, 증거 데이터에 대한 정보, 분석에 대한 정보를 총 2단계인 『M32-03 폰파일시스템으로 재구성』, 『M32-04 통신사별 파일포맷 관련 Properties구성』으로 구분하여 6하 원칙에 따라 작성한 후, 사건 종료 이후라도 증거 데이터의 절차 연속성에 따른 입증 및 재검증이 필요할 경우를 대비하여 관리 보관한다.



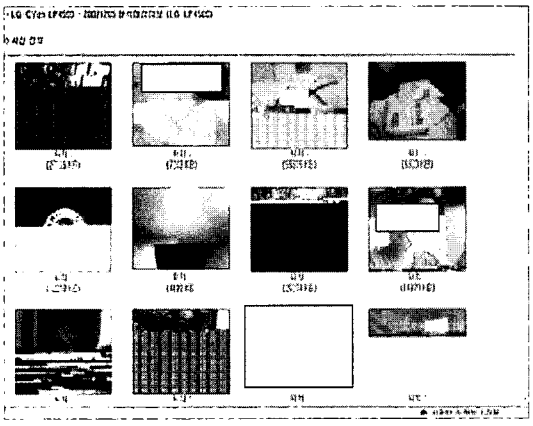
[그림 14] 통신사별 파일 포맷 Property



[그림 15] Property 프로그램 분석 실행



〔그림 16〕 Property 프로그램 분석 실행 결과



〔그림 17〕 Property 프로그램 복원 결과

이와 같은 방식과 달리 기존 NIST 방식의 구현 절차 모델 방식으로 구현 할 경우에는 크게 3가지 증거 데이터 획득의 어려움이 도출될 수는 결과를 알 수 있었으며, 〔표 9〕와 같이 비교 할 수 있다.

1) 조사자의 휴대폰(A사-LP4500)경우 휴대폰은 정상 작동은 되었지만 JTAG 핀맵인 포트 확인이 불가하여 JTAG 포트의 신호 체계를 통한 데이터 획득에 어려움이 발생한 경우

2) 조사자의 플래시 메모리의 사본이미지가 결함이 발생하여 삭제영역에서 조사자의 결정적인 증거 데이터가 발견되더라도 무결성의 입증이 어려운 경우

3) 조사자의 데이터를 분석·복원 시 대상 파일 시스템 구조가 일반적인 파일 시스템 구조와 상이하여, 일반적인 디지털 포렌식 기법 중의 하나인 파일 시그네이쳐 방식을 통하여 복원하는 방식의 적용이 불가능한 경우

〔표 9〕 검증 시나리오 절차 모델 비교표

단계	E-Finder 절차 모델	NIST 절차 모델	절차 적용 여부
1	사전준비단계	존재하지 않음	X
2	이미징 및 1차 해쉬 함수 구현단계	존재하지 않음	X
3	차폐관리단계	존재하지 않음	X
4	현장보존단계	보존	○
5	조사 및 인식 단계	현장 확인	○
6	문서화 단계	기록	○
7	논리적인 데이터 획득 단계	수집	○
8	물리적인 데이터 획득 단계	수집	○
9	E-F 물리적인 데이터 획득 단계	존재하지 않음	X
10	증거보관 및 이송 단계	보관 및 이송, 차폐관리	○
11	검사 및 추출 단계	검사	○
12	증거 데이터 분석 단계	분석 · 복원	○
13	2차 해쉬 함수 구현 및 복원 단계	존재하지 않음	X
14	결과 보고서 단계	보고서	○
15	보존 및 증거 관리 단계	존재하지 않음	X

VI. 결 론

본 논문에서는 모바일 포렌식의 무결성 보장을 위한 효과적인 방법으로 15단계의 새로운 E-Finder 모델 절차를 수립하였다. 다음 사항은 본 논문에서 얻어진 결과물에 관한 주요 내용이다. 첫째, E-Finder 절차 모델은 모바일 포렌식 수사 절차상 MD5 해쉬 함수를 적용한 데이터에 결함이 발견될 경우 폐기처분할 수밖에 없는 주요 증거 데이터에 대하여 절차 모델을 통한 증거 능력을 확보하는 방안을 수립하였다. 즉, 기존에는 사본 이미지 전체를 이미지화하여 해쉬 함수를 적용하였지만, 본 논문은 삭제 영역의 훼손 여부를 가려냄으로써 증거 능력으로 인정받을 수 있었다. 이와 같이 15단계의 E-Finder 모바일 포렌식 절차를 수행하게 됨으로써 데이터의 훼손여부에 따라 기존의 삭제 미해결 사건이나 미제출로 인한 해결 불가능한 사건에서도 증거로서의 활용 가능성을 높일 수 있었다. 둘째, 새로운 Serial(UART) 통신을 이용하는 플래시 메모리 증거 획득에 대한 절차 모델에 관하여 연구하였다. 기존 Sync통신을 이용한 증거 획득 방법은 논리적인 획득으로 활성상태에서 메모리의 데

이터를 획득하기 때문에 삭제된 데이터의 복원은 불가능하였지만, 새로운 Serial(UART) 통신 기법은 S/W구현 방식을 통한 물리적인 데이터 획득 방식으로서 새로운 휴대폰이 출시되더라도 손쉽게 물리적인 데이터를 획득할 수 있어, E-Finder절차에 구현되었다. 셋째, E-Finder 모델 절차를 모의시나리오 사례에 적용하였다. 새로운 모바일 포렌식 통제 방법을 실제적으로 적용하기 위해서 가상의 모의시나리오 케이스를 수립하고 동일하게 NIST 방식과 15단계의 통제 방법을 비교하여 단계별로 데이터의 무결성을 보장할 수 있도록 구현해 보았다.

이와 같이 모바일 포렌식의 무결성을 확보하기 위한 효과적인 방법에도 불구하고 존재하는 연구의 한계점과, 그에 따른 향후 연구 방향은 다음과 같다.

첫째, 현재 국내 휴대폰의 작동 방식은 CDMA방식으로 미국 방식이다. 현재 글로벌화 되고 있는 국내 환경에 대비하여 향후 GSM방식의 휴대폰에 대한 통제 방안의 연구가 시급한 실정이다. 둘째는 국내 실정에 적합한 모바일 포렌식의 플랫폼의 수립이다. 플래시 메모리의 경우 데이터를 분석하기 위해서는 플래시 메모리에서 사용하는 파일 시스템을 알아야 하는데 EFS, EFS2, TFS와 같이 논리적인 파일 시스템간의 정보는 제조사의 주요 정보로 분류되어 공개되지 않고 있고 파일 시스템은 각 제조사의 Know-How에 따라 변형하여 사용하고 있어 파일시스템 또한 휴대폰 모델마다 분석되어야 한다.

참 고 문 헌

[1] 김기환, 박대우, 신용태, "모바일 포렌식에서의 무결성 입증방안 연구," 한국정보보호학회 하계학술대회발표집, pp. 37-46, 2007년 6월.

[2] 김용호, "디지털증거 확보를 위한 파일 삭제 탐지 모델," 박사학위논문, 경기대학교, 2007년 8월.

[3] 성진원, 김권엽, 이상진, "국내 휴대폰 포렌식 기술 동향," 정보보호학회지, 18(1), pp. 63-69, 2008년 2월.

[4] 이경민, "모바일 포렌식을 위한 CDMA 휴대폰의 데이터 획득 및 분석에 관한 연구," 석사학위논문, 동국대학교, 2006년 12월.

[5] 이성진, "디지털 증거분석 표준 가이드라인에 대한 연구," 치안정책연구소, pp. 11-13, 2007년 7월.

[6] 이광열, 최윤성, 최해랑, 김승주, 원동호, "현행 증거법에 적합한 디지털 포렌식 절차," 정보보호학회지, 18(3), pp. 82-90, 2008년 6월.

[7] 오기두, "형사절차상 컴퓨터 관련 증거의 수집 및 이용에 관한 연구," 박사학위논문, 서울대학교, 1997년 2월.

[8] 임동환, "디지털 환경하에서 효율적인범죄수사 및 증거분석을 위한 포렌식 프로세스 모델연구," 박사학위논문, 한세대학교, 2007년 12월.

[9] 전상덕, "정보보호 증적 확보를 위한 디지털포렌식 개요," 감리뉴스, 2008년 4월.

[10] 탁희성, "형사절차상 디지털 증거에 관한 연구," 형사정책연구원, pp. 137-140, 2002년 2월.

[11] 홍성경, "디지털 포렌식 절차 모델에 관한 연구," 석사학위논문, 한남대학교, 2006년 2월.

[12] Anup Ramabhadran, "Forensic Investigation Process Model For Windows Mobile Devices," Tata Elxsi Security Group, June 2007.

[13] C.H. Park, "Phone Extractor User Manual," UNET Information Technology, Oct. 2008.

[14] G. Palmer, "A road Map for Digital Forensics Research-report from the first Digital Forensics Research Workshop. Technical Report DTR-T001-01 Final," Air Force Research Laboratory, Aug. 2001

[15] M.G. Noblett, M.M. Pollitt, and L.A. Presley, "Recovering and examining Computer Forensic Evidence," Forensics Science Communication, vol. 2, no. 4, pp. 2-3, Oct. 2000.

[16] W. Jansen and R. Ayers, "Guidelines on Cell Phone Forensics," NIST, Draft Special Publication 800-101, Sep. 2007.

[17] S.Y. Willassen, "Forensic analysis of mobile phone internal memory," IFIP, vol. 194, pp. 191-204, June 2005.

〈著者紹介〉

김 동 국 (Dong Guk Kim) 정회원
1991년 8월: 국립 서울산업대학교 전자계산학과 이학사
1998년 2월: 홍익대학교 국제경영대학원 회계학과 경영학석사
2009년 2월: 국립 서울산업대학교 IT정책전문대학원 산업정보시스템 전공 공학박사
2006년 ~ 현재: (주)에이쓰리시큐리티 컨설팅사업부 수석 컨설턴트
〈관심분야〉 개인정보보호, 모바일 포렌식, 전산감사, 산업보안, 위험관리, SROI

장 성 용 (Seong Yong Jang) 정회원
1980년 2월: 서울대학교 산업공학과 공학사
1982년 2월: 서울대학교 산업공학과 공학석사
1991년 2월: 서울대학교 산업공학과 공학박사
1987년 ~ 현재: 국립 서울산업대학교 산업정보시스템공학과 교수
〈관심분야〉 시뮬레이션, e-비즈니스, 프로젝트 경영, SCM, TOC

이 원 영 (Won Young Lee) 정회원
1978년 2월: 서울대학교 산업공학과 공학사
1983년 2월: 미국 오하이오주 오하이오 주립대학교 산업공학과 졸업 (M.S.)
1990년 2월: 미국 켄터키주 루이빌 대학교 산업공학과 졸업 (Ph.D.)
1991년 8월 ~ 현재: 국립 서울산업대학교 산업정보시스템공학과 교수
〈관심분야〉 데이터베이스, 인공지능/전문가시스템

김 용 호 (Yong Ho Kim) 정회원
2002년 2월: 광운대학교 정보통신학과 공학석사
2008년 8월: 경기대학교 정보보호학과 이학박사
2002년 ~ 2007년: 경찰청 사이버테러대응센터 연구원
2009년 ~ 현재: 경기대학교 산업기술보호특화센터 산업보안학과 연구교수
〈관심분야〉 시스템 포렌식

박 창 현(Chang Hyun Park) 정회원
1993년: 동국 대학교 컴퓨터 공학 석사
2004년 ~ 2008년: 대검찰청 보안 기술 자문역
2009년 ~ 현재: 모바일 포렌식 전문 기업 (주)유넷정보통신 대표이사
〈관심분야〉 정보보호, 디지털 포렌식, 모바일 포렌식, 모바일 장비 제어