휴대폰 압수수색 표준절차와 포렌식 무결성 입증

정회원 이 규 안*, 박 대 우**°, 신 용 태*

A Study on Forensic Integrity Proof Standard a Cellular Phone Confiscation Criminal Investigation

Gyu-an Lee*, Dae-woo Park**°, Young-tae Shin* *Regular Members*

요 약

범죄에 사용된 휴대폰의 증거는 수사와 법정판단의 중요한 자료가 된다. 다양한 휴대폰의 종류와 모델, 통일되지 않은 파일 포맷을 사용하여 범죄 증거를 수집하고 분석하는 과정에 많은 어려움이 있다. 또한 압수 수사현장에서 휴대폰에 대한 압수수색 과정에서부터 포렌식 자료의 무결성 추출까지의 절차상 표준화가 되어 있지 않아, 법정에서 채택할 수 없게 된다. 본 논문에서는 휴대폰의 압수 수색 절차를 표준화한다. 표준 절차에 의한 범죄 현장에서 휴대폰 압수 수색 자료의 무결성을 확보 하기위한 전파차단봉투와 이동용 전파차단장치를 사용한다. 압수된 휴대폰의 증거 자료를 분석하고, 무결성 훼손 실험을 통해 무결성을 검증하고, 휴대폰 압수수색 절차에 대한 문제점 및 대책을 제시함으로 모바일 포렌식의 발전에 기여하고자 한다.

Key Words : Digital Forensic. Mobile Forensic, Evidence Analysis

ABSTRACT

The proof of a cellular phone used to a crime important data of a criminal investigation and legal judgment become. A lot of on a process use the file format that do not become that is kind of various cellular phones and model pipe, and collect criminal proof, and to analyze be difficult. Also, standardization is not made, and can be adopted on procedures from confiscation search processes regarding a cellular phone to integrity extractions of Forensic data in courts in the confiscation criminal investigation spots. Standardize confiscation search procedures of a cellular phone at these papers. Use a radio waves interception envelope and radio waves interception device for a movement which a security does integrity of criminal on-site cellular phone confiscation search data by standard procedures, and was devoted to. Analyze corroborative facts of a cellular phone seized, and verify integrity, and present problems regarding cellular phone confiscation search procedures and measures, and will contribute in development of Mobile Forensic through integrity damage experiment.

I. 서 론

모바일이란 컴퓨팅과 네트워킹 기능의 이동성을 부여한 장비를 말한다. 이동성을 부여한 모바일 단말기 중에서 휴대폰이 가장 일반적인 장비이다. 대한민국 휴대폰 가입자는 2007. 7월을 기준으로 4천 2백 만 명[1]을 초과하여 국민 1인당 1대의 휴대폰을 소유하고 있는 실정이다. 또한 휴대폰의 기능도 다양해져, 처음 휴대폰이 출시되었을 당시 제공되었던 음성통화와 메시지통화(SMS: Short Message Service)

※ 본 연구는 숭실대학교 교내연구비 지원으로 이루어졌습니다.
* 숭실대학교 대학원 통신연구실, **호서대학교 벤처전문대학원(prof1@paran.com)(° : 교신저자)
논문번호 : KICS2008-01-029, 접수일자 : 2008년 1월 15일, 최종논문접수일자 : 2008년 5월 27일

를 하던 것이 현재는 화상통신, 컬러메일, 게임, MP3, 전자다이어리, 전화번호, 스케줄, 카메라, 동영상 촬영 등 거의 모든 컴퓨터의 기능을 보유하고 있을 뿐만 아니라, 멀티미디어화 되고 소형화 되었다[2].

이러한 휴대폰의 특징으로 인하여 휴대폰이 범죄에 이용되어지고 있으며, 이 결과 휴대폰에 저장된 디지털 자료는 수사와 법정의 증거자료로 활용된다[3].

모바일 포렌식에는 무선 네트워크의 특성상 언제나 통신이 연결 가능한 환경에 노출되어 휴대폰의 전원이 켜져 있는 상태에서는 메시지(SMS)가 수신되거나, 휴대폰의 통화 신호가 유입된다. 이때 휴대폰 소지자가 통화 동작을 취하지 않으면 부재 중 신호가 유입되는 등 사건이 진행되었던 당시의 디지털 증거는 변경될 가능성이 존재하고, 이러한 디지털 증거의 변경은 모바일 포렌식의 무결성을 훼손하게 되어 증거의 가치를 감소시키거나 혹은 법정에서 증거로서 채택할 수 없는 경우에 이르기도 한다.

법정 근거자료로써 이러한 무결성을 확보하기 위해, 본 논문에서는 범죄발생 현장 혹은 압수수색 과정에서 휴대폰에 저장된 모바일 포렌식의 무결성 훼손에 관한 문제점을 해결하기 위한 절차상의 압수수색과 모바일 포렌식을 위한 압수수색 현장에서의 해결방안을 제안하고, 무결성을 검증하여 법정근거 자료로 채택되도록 증명을 해 보이겠다.

Ⅱ. 관련 연구

휴대폰의 플래시 메모리의 경우 기본이 1GB급으로 한글문서 A4용지로 5만장의 분량이다. 휴대폰의 메모리에는 통신의 기록뿐만 아니라 범죄에 사용되는 자료 저장이 가능한 플래시 메모리가 장착되어, 활용하는 곳으로는 교통카드 또는 휴대폰의 보조기억장치, 카메라 저장장치와 겸용으로 사용하면서 디지털 증거를 은닉할 수 있고, 현재 16GB급 메모리가 양산 되고 있다.

2.1 모바일 포렌식

2.1.1 모바일 포

모바일 포렌식을 적용하기 위한 디지털 자료의 종류를 구분하는 학설의 구분은 없다. 하지만 현장에서 경험하고 실무에 적용하기 위한 임의의 분류는 다음과 같다.

1) 휴대폰(Cell Phone)의 음성 및 SMS 기록 자료
2) PDA(Personal Digital Assistant)의 자료
3) Digital Voice Record의 자료
4) 디지털카메라와 휴대폰의 사진 및 동영상 자료
5) 차량, 선박, 기차, 비행기 등 이동기기들의 전자기록 자료
6) 이동저장장치에 부가된 전자자료 등

2.1.2 모바일 포렌식의 특징

모바일 장비는 디지털 장비 중에서 이동성을 부여한 것이고, 대표적인 것으로는 휴대폰, PDA, 디지털 녹음기, 디지털 카메라와 이동기기 등에 임베디드 시스템이 활용되는 분야라고 할 수 있다. 특히 휴대폰은 전세계적으로 가장 많이 사용하는 모바일 장비이고, 무선 네트워크가 구성되어 있으므로 모바일 포렌식에서 압수수색 등 절차 상 가장 유의하여야 하는 분야다.

2.2 모바일 포렌식을 위한 장치 및 도구

모바일 포렌식을 위해 현재 사용되고 있는 장치 및 도구로는 은닉된 모바일 기기에 대한 탐지를 할 수 있는 금속 탐지기, 압수되거나 임의 제출된 모바일 기기를 공중파로부터 차단하기 위한 전파 차단 봉투, 모바일 기기에서 데이터를 추출하는 장치 및 추출된 데이터로부터 필요한 정보를 분석할 수 있는 분석 툴로 이루어진다.

2.2.1 전파 차단봉투

휴대폰을 압수 수색하는 과정에서 사용하는 전파 차단봉투는 그림 1과 같이 겉표지에 압수수색을 집행하는 기관명과 압수수색 대상, 그리고 인적사항을 기재하도록 한다. 내부로는 충격을 방지할 수 있는 버블 보호막을 1차로 구성하고, 2차로 전파를 차단할 수 있는 모직에 구리나 니켈로 도금된 실크 메시 장치를 하였다[4].

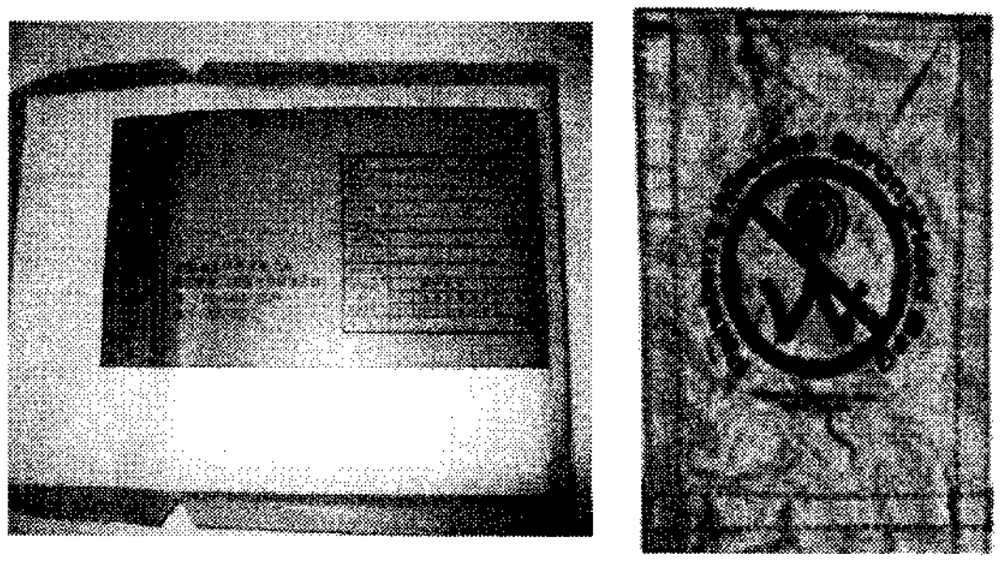

그림 1. 국내외 전파차단봉투
Fig. 1. Anti-radio wave envelope

2.2.2 이동용 전파 차단 장치

전파의 유입으로 인하여 디지털 증거의 무결성이 훼손되는 사례를 방지하기 위하여 그림 2와 같이 (주)F사에서는 휴대폰을 분석하기 전에 전파 차단 장치를 별도로 제작하여 휴대폰 분석 장치 속에 포함하여 판매하고 있다. 이러한 전파 차단장치는 제작사에서 전파의 차단지수를 측정하고 이를 이용하여 전파 유입으로 인한 디지털증거의 훼손을 방지하고 있다.

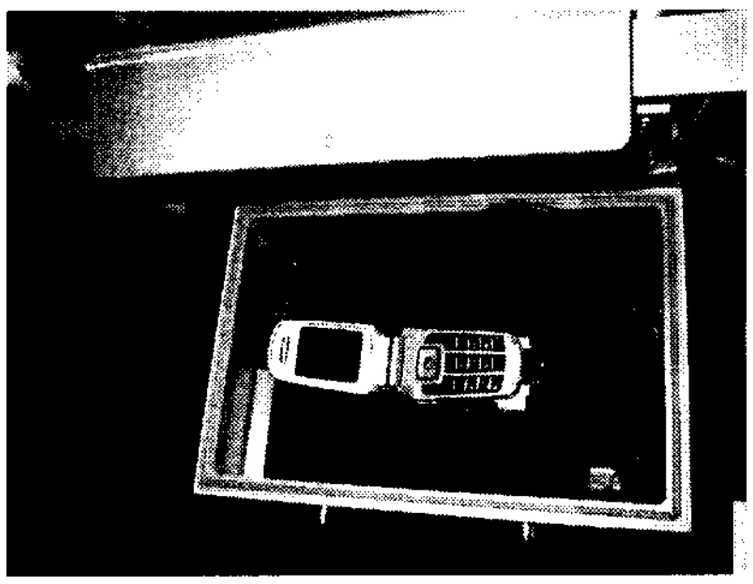

그림 2. (주)F사의 이동용 전파차단장치
Fig. 2. Portable anti-radio wave equipment of F corp.

2.2.3 전파 차단실

전파 차단실내에서는 전파는 완전히 차단되어야 하며, 휴대폰의 접점불량을 점검하기 위하여 확대경이 설치되어야 하고, 전원을 충전하기 위한 전원 충전 장치, 휴대폰으로부터 이미지를 추출하기 위한 이미지 추출 장치 등을 구비하여야 한다. 그림 3과 같이 전파 차단실은 전파의 차단을 위하여 창문마다 보호 장치를 하여야 하고, 출입문도 2중화 하는 등 철저하게 전파의 차단 방안을 강구해야 한다.

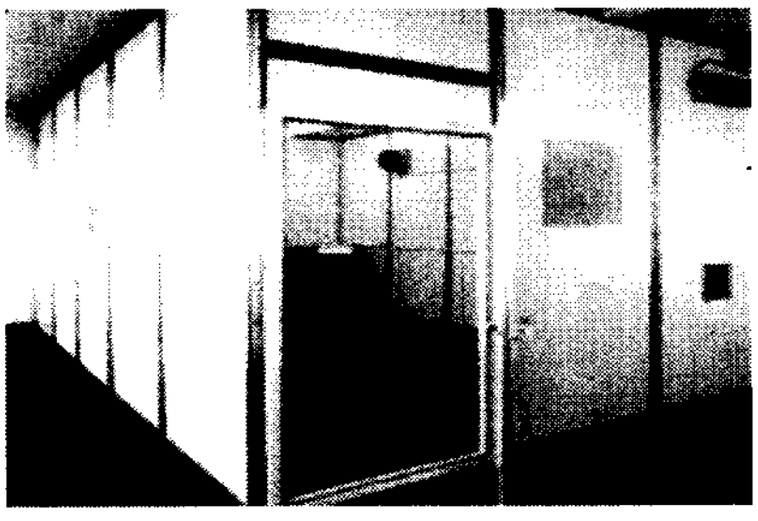

그림 3. 전파 차단실
Fig. 3. Anti-radio wave chamber

2.3 모바일 포렌식을 위한 자료 추출 기법

현재 모바일 포렌식을 위해 현장에서 사용하고 있는 모바일 포렌식 기법 중, 휴대폰의 디지털 증거자료의 추출 및 분석기법은 3가지로 구분 할 수 있다.

2.3.1 SYN 통신을 이용하는 방법

휴대폰 제작사에서 제공하고 있는 PC link 기능을 이용하여 데이터를 수집하는 방법으로서 휴대폰의 SRAM과 플래시메모리 일부에서 데이터를 추출하는 기법이다. 그림 4와 같이 휴대폰의 SRAM영역에 저장되어 있는 데이터를 수집할 수 있는데 이와 같은 수집기법은 단점은 미할당 영역에 남아 있는 데이터를 수집 할 수 없고, 여기에 논리적인 영역의 데이터를 수집하기 위하여 별도의 통신방법을 이용하여 플래시 메모리영역에 산재되어 있는 일부 자료를 수집할 수 있으며 전체 자료 수집을 위해서는 기술적인 보완이 필요하다.

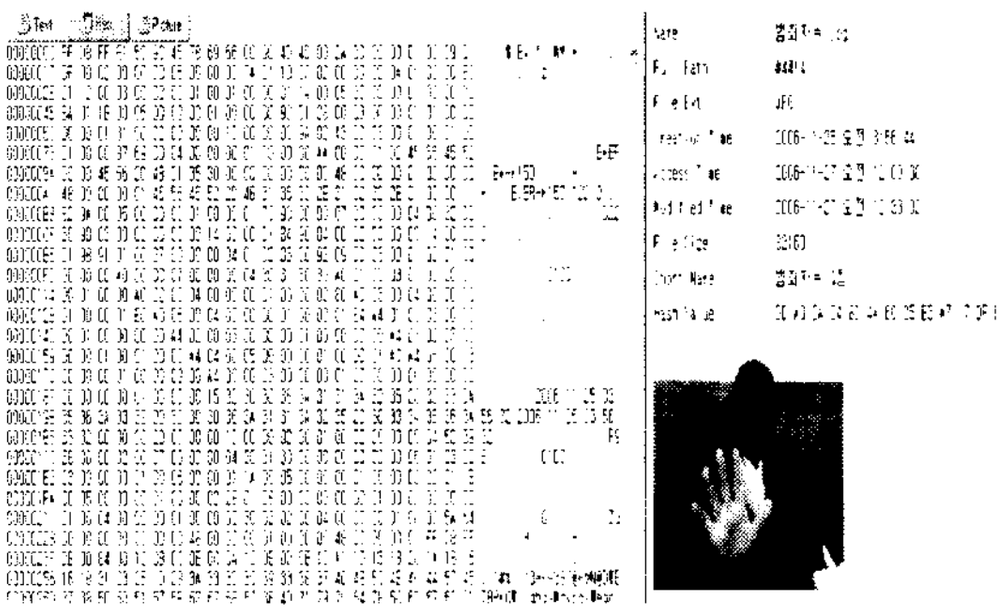

그림 4. (K)사 핸드폰의 사진 헤드 포맷
Fig. 4. Hea format, photo stored in a cell phone manufactured by K. Corp.

2.3.2 JTAG 에뮬레이터를 이용하는 방법

JTAG 포트를 이용하여 SRAM과 플래시메모리 부분까지 데이터를 추출하는 방법이다. 각 제작사 및 제품별로 휴대폰의 PCB(Printed Circuit Board)에 JTAG의 통신을 위한 포트가 존재하는데 이러한 포트를 찾아서 모든 영역의 데이터를 덤프하는 기법으로 안테나 차단이 되는 등 디지털증거의 무결성을 보장하고 감춰진 디지털자료를 추출하는 기법으로 연구가 진행 중이다[4].

2.3.3 메모리 칩을 분리하는 방법

PCB에 장착된 플래시 메모리를 분리하여 데이터를 추출하는 기법으로 휴대폰에 고의 또는 부주의로 인하여 파손되거나 동작이 불가능할 경우에 사용하는 방법이다. 물리적으로 분리하여 이미지를 추출하기 때문에 분석이 종료하고 난 후에 휴대폰의 정상적인 동작을 보장하기 어렵다. 하지만 수사상 매우 중요한 데이터의 필요성과 휴대폰 사용자가 동의를 할 경우 등 특수한 조건하에서 추진된다[6].

Ⅲ. 모바일 포렌식의 수행 절차

3.1 압수수색 중 휴대폰의 증거 확보

범죄 현장에서 범죄에 사용된 휴대폰은 대용량 소형화된 장비로서 증거 자료의 은닉성이 뛰어나며, 현재 16GB급 메모리가 활용되어 데이터를 은닉하게 된다. 따라서 수사 요원들은 범죄 증거의 가능성이 높은 휴대폰의 증거 확보를 위한 압수 수색을 하여야 한다.

3.2 휴대폰의 압수수색 표준절차 및 전파차단

그림 5처럼 압수 수색한 휴대폰의 전파 차단은 무결성을 입증하는 관건이 되고 있다. 휴대폰의 경우 소형저장장치의 효율성을 높이기 위하여 각 회사별로 별도의 메모리 저장 공간을 사용한다. 메시지의 경우 100개정도의 저장 공간을 할당하고, 그 이상의 데이터는 순번대로 삭제하는 방법을 활용한다.

이때 압수수색을 진행 중이거나 분석을 위하여 휴대폰을 동작시킨다면 기지국 서버에 저장중인 메시지, 음성신호, 통화신호등이 휴대폰에 유입되어 휴대폰에 저장된 오래된 순서대로 디지털 증거들을 삭제하는 등 무결성을 훼손하게 된다. 그러므로 휴대폰 등 무선 네트워크를 사용하는 모바일 장비는 전파의 차단이 관건이 된다.

휴대폰에서 압수수색을 진행하기 전에 전원이 켜져 있는 상태라면 휴대폰의 사용자나 입회인에게 현재 상태를 확인한 후, 전원을 끄고, 전파 차단되도록 되어있는 보존봉투에 밀봉 보관하여 그 내용을 기재한 후 서명을 받도록 한다[7].

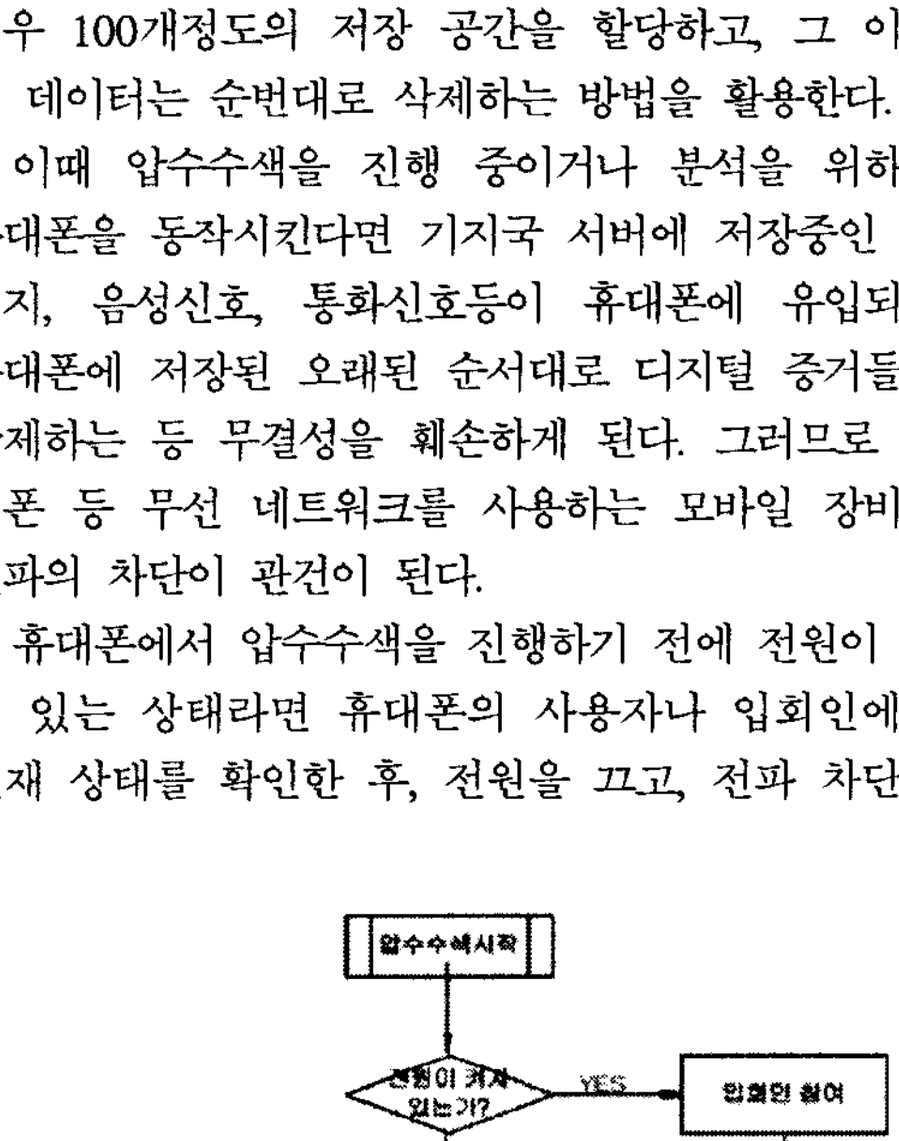

그림 5. 모바일 포렌식 압수·수색 표준 절차
Fig. 5. Seizure standard procedure for mobile forensic

이때 휴대폰의 제작사에서 제공하는 통신 프로토콜을 이용하여 컴퓨터에 휴대폰의 정보를 전송할 수 있으므로 컴퓨터와 통신여부를 확인한 후 통신 케이블, 통신 프로그램, 외장형 메모리 등도 압수하여 전파 차단 봉투에 밀봉하고 그 내용 등을 상세히 기재하여야 한다.

3.2.1 전파 차단 봉투, 이동용 전파 차단 장치 이용

만약 전원이 꺼져있는 휴대폰이라면 외관 상태와 휴대폰의 동작 상태 등을 휴대폰의 사용자에게 확인 후에 사용자와 함께, 사진을 찍은 후에 전파 차단 봉투에 밀봉 보관하고 그 내용을 기재한다.

전파차단봉투는 파라반사에서 제공하는 봉투가 있으나 이를 모든 수사 현장에 공급하기는 어려움이 있으므로 밀봉상태를 확인할 수 있도록 개폐여부를 구분 가능한 1회용 접착방식을 사용하고 그 개폐 사용여부를 보관봉투의 겉봉에 기재한다.

3.2.2 전파 차단실 이용

압수·수색된 휴대폰은 전파 차단봉투에 의하여 밀봉된 후 보관실로 인수인계를 하게 된다. 담당자는 밀봉된 상태에서 개폐된 흔적 여부를 확인한 후 인수인계서에 서명하고 보관하게 되고, 분석을 위하여 분석 담당자에게 인계 된다. 분석 담당자는 전파의 유입이 차단되는 장치 혹은 전파 차단실 내에서 분석 시작 시간, 분석 과정 등을 기재하면서 분석을 진행하여야 한다[8].

3.3 휴대폰의 파일 포맷 분석

휴대폰은 제작사 별로 기종과 사용하는 운영체계 및 웹 브라우저 및 파일 포맷을 분석 하여야 한다. 물리적인 분석방법과 파일 포맷을 기본적으로 이해하고 적용하는 것이 필요하다.

즉 휴대폰과 같은 모바일 기기는 모바일 제조회사와 메모리 제조회사별로 서로 다른 특성을 가지고 있다. CDMA폰을 사용하는 국내의 휴대폰은 퀄컴사의 기본 기술 위에 각 회사에서 자체 개발한 운영 프로그램과 애플리케이션 등을 기본 메모리를 이용하여 사용할 수 있도록 정보를 저장하므로 파일구조와 인터페이스부분은 각 회사별로 서로 상이하고, 이러한 프로그램을 펌웨어로 제작하여 운용하는 관계로 모바일 포렌식 증거 자료를 추출하는 일에는 많은 어려움이 있다[9].

3.4 휴대폰의 파일 증거 자료 분석

모바일 기기는 여러 기업에서 개발되어 표준화된 방법과 절차가 존재하지 않는다. 따라서 모바일 포렌식 자료 분석가는 리눅스에서 쓰이는 임베디드 프로그래밍을 습득하고, 표준 통신 프로토콜이 존재하지 않으므로 회사에서 제공한 통신 프로토콜을 이용하여 분석하기도 하지만 이는 삭제되거나 변조된 디지털 증거를 추출하고 분석할 수 없기 때문에 무선 네트워크, 파일구조, 프로그래밍을 이해하여, 물리적으로 추출하고 분석하여야 한다.

이때 추출된 데이터는 헥사 값을 가진 일반 비트들의 나열이므로 디지털 자료에서 수사에 필요한 사진의 경우에는 사진 포맷의 헤더 값을, 음성인 경우에는 음성 포맷의 헤더 값을 알고 접근해야 한다[10].

3.5 휴대폰의 포렌식 문제점 및 해결방안

다양한 종류의 모바일 기기를 압수수색하고 증거를 추출하기 위한 표준화된 절차와 방법이 없는 현실에서 무결성을 입증하기 위한 휴대폰의 모바일 포렌식 문제점은 모바일 기기의 특징이 무선 네트워크를 통하여 끊임없이 접속을 시도한다는 점이다.

이는 휴대폰의 경우에 개통이 되어 있는 통화중이 아닌 상태에서는 대기모드로 되어 있으며, 이때 휴대폰은 기지국에 대하여 자신의 슬롯을 감시하고 있다. 이때 매 슬롯마다 실어오는 General Page Message를 확인하다가 자신을 호출하는 정보를 수신하게 되면 휴대폰은 통신 절차에 들어가게 되는데 이때 통화신호, 메시지 등이 유입되게 된다. 이러한 문제점을 이해하고 대처할 수 있는 모바일 포렌식의 현실에 대한 문제점을 표로 표현하면 표 1과 같다[11].

표 1. 모바일 포렌식의 문제점과 해결방안
Table 1. Problems and solutions of mobile forensic

구분	문제점	해결방안	비고
전문수사관	전문화된 교육 부재	교육기관 양성	협회지원
표준 절차	국내기술에 적합한 표준 기술 부재	협회를 통한 표준화 연구	연구개발
표준 장비	국내3개사 연구중, 국외기술 도입 불가	국가의 재정적인 지원	연구개발
전파차단	일시 보관된 정보 입력으로 무결성 훼손	전파 차단장치로 정보 유입 차단	연구개발

Ⅳ. 압수 휴대폰의 무결성 입증방안

4.1 전파 차단봉투 실험

그림 6과 같이 전파 차단 봉투의 겉표지에는 수사기관을 표시할 수 있는 마크와 수사에 관계된 사항을 기재할 수 있는 메모 기능이 부착되어 있다.

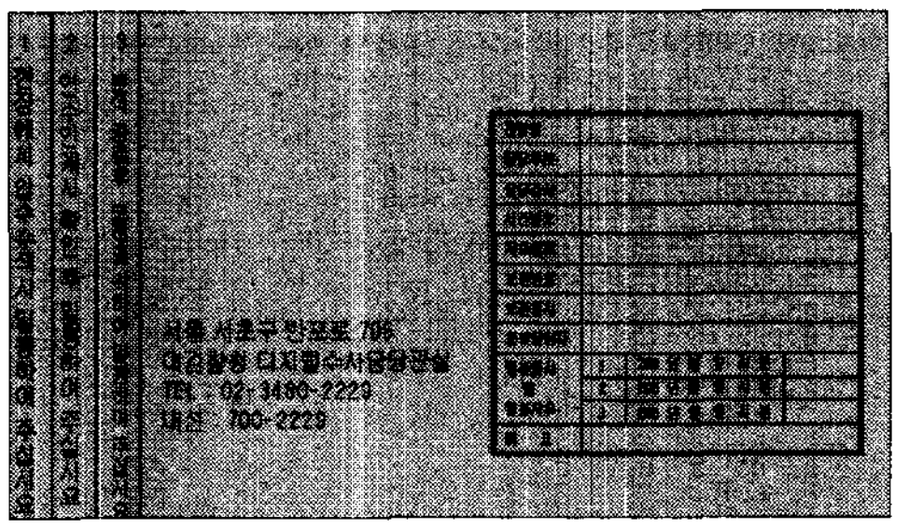

그림 6. 전파 차단 봉투
Fig. 6. Anti-radio wave envelope

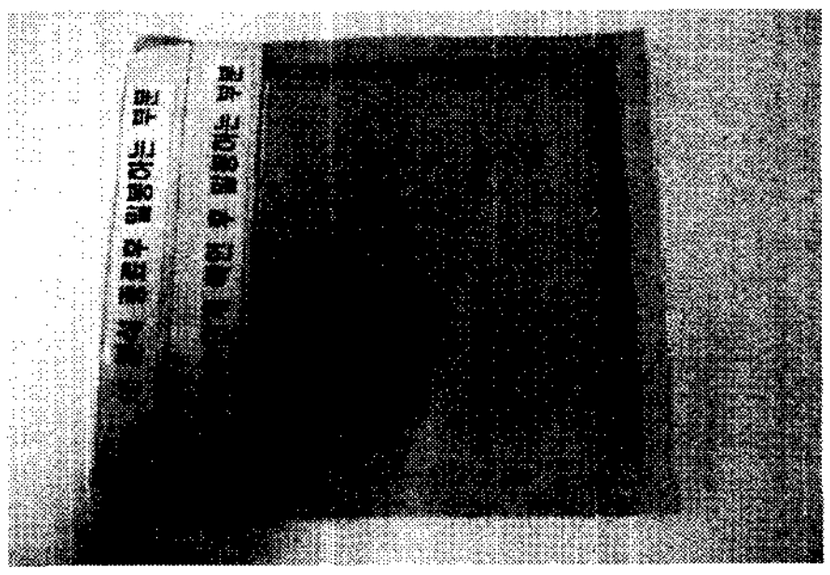

그림 7. 현장 휴대폰 압수 밀봉후 인수인계단계 봉투 상태
Fig. 7. Transition of seized cell phone sealed in envelope

4.1.1 전파 차단봉투 실험 준비

전파차단봉투는 일반적인 모직이나 실크 등에 니켈, 구리 등의 산화물을 도포하거나, 그물형식으로 만들어 2중화한다. 이 장치는 전파 차단봉투의 위아래 2중화된 부분과 서로 겹칠 수 있도록 되어 있으므로 밀봉된 상태를 개봉하기 전에는 전파가 유입되지 않도록 하였다. 그림 8과 같이 강력 접착 테

모델명	최고 차폐효과	최저 차폐효과
SCREEN Ⅱ	121.5 dB	91.5 dB
(Ni25%, Cu35%, Resin40%, 0.2t)	(200.5 MHz)	(1491.1 MHz)

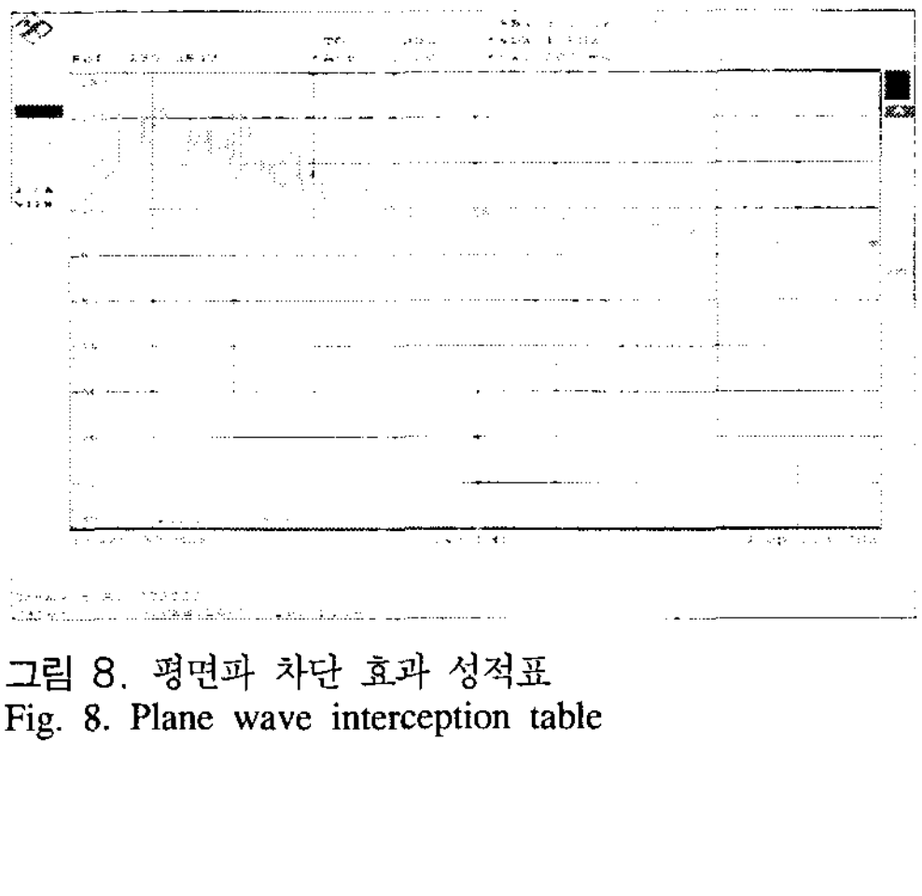

그림 8. 평면파 차단 효과 성적표
Fig. 8. Plane wave interception table

입을 사용하여 3회 밀봉 과정이 필요하다. 처음에는 모바일 관련 장비를 압수수색하는 과정에서 밀봉을 하고, 그 다음에는 물품 담당자에게 전달하는 인수인계과정에서 발생할 수 있고, 마지막으로 분석을 위하여 개봉을 한 후 보존을 위한 밀봉으로 3회에 걸쳐 개폐작업을 진행됨을 알 수 있다.

4.1.2 압수 휴대폰의 전파 차단봉투 실험

전파 차단 봉투를 이용하여 가장 많이 사용되는 제작사 별로 휴대폰을 임의 선정하여 실험을 해보았다. 휴대폰의 전원은 켜진 상태로 전파 차단 봉투에 삽입한 다음 밀봉을 하여 컴퓨터의 메신저 기능을 이용하여 메시지 및 통화를 시도하였다.

실험 결과 표 2와 같이 휴대폰에는 메시지가 전혀 유입되지 않았으며 통화음도 수신되지 않았다. 다시 밀봉된 전파 차단 봉투를 개봉한 후 휴대폰을 꺼내놓은 즉시 바로 메시지는 유입되었고, 통화음은 수신되지 않았다.

표 2. 메시지 및 통화 실험 결과
Table 2. Result of message and telephone call test

실험내용 / 회사	메세지	통화신호	비고
S 사	유입 불가	차 단	
L 사	유입 불가	차 단	
K 사	유입 불가	차 단	

4.2 전파 차단실 실험

4.2.1 전파 차단실 실험 환경

휴대폰 개발사에서 실험실에서 사용하고 실험실을 빌려 휴대폰의 분석을 위한 전파 차단실을 구성하고 실험을 실시한다. 그림 8과 같은 전파차단 효과가 있는 실험실은 무엇보다 전원을 통한 전파 유입, 출입문을 통하여 분석자가 출입을 할 때 전파가 유입될 수 있으므로 반드시 2중화된 출입문 등을 구비해야 한다.

4.2.2 전파 차단실 실험

(주)S사의 전파 차단실에서 실험한 결과 전파의 유입은 발생하지 않았다. 단 이 실험은 수사기관에서 실시한 실험은 존재하지 않으므로 휴대폰을 제작하는 회사의 도움으로 실시되었다.

4.3 전파 차단 봉투와 차단실 연계 실험

휴대폰에 대한 인수인계과정이 적절하게 되었는지 확인하기 위하여 GPS표준시간을 적용하여 시간 스템프를 확인한 후 1시간, 3시간, 5시간 후의 메시지 유입 및 통화신호에 대한 데이터 유입 여부를 확인하였다.

그림 9와 같이 일정시간이 경과한 다음 데이터의 유입여부를 확인 결과, 전파 차단실에서 모바일 장비의 분석을 진행하여 디지털증거의 무결성을 입증할 수 있게 되었다.

하지만 전파 차단실의 문을 여는 순간 데이터의 유입이 발생할 수 있으므로 휴대폰에 대한 분석을 시작하기 전에 전원부의 동작 전에 전파 차단실을 완전 폐쇄함으로 디지털 자료의 유입을 막고, 최소한 이미지 추출이 종료되고 휴대폰의 동작을 종료(전원 차단)가 되기 전까지 차단실 내외에 알람을 설치하여, 문을 개방하는 등의 행위가 일어나지 않도록 주의하여 실험 하였다.

그림 9. 분석 전·후의 전파 유입여부를 확인하기 위한 국제표준시계
Fig. 9. International Standardized Clock used in order to identify the inflow of radio wave before and after the analysis.

4.4 압수 휴대폰의 파일 증거 실험 전·후 분석

현장에서 휴대폰의 압수수색을 진행하는 과정에서 일어날 수 있는 상황을 재현하기 위하여 휴대폰의 전원을 켜진 상태에서 메시지를 발송하고, 그 결과 추출된 디지털 증거에서 메시지가 어느 부분이 삭제되는지를 살펴보았다.

그 결과 새로운 메시지의 유입은 회사의 정책에 따라 상이하지만 보통 비어있는 공간에 채워지는 순서대로 진행하고, 기본 용량을 모두 채웠을 경우에는 메모리 부족이라는 문구를 표시한다. 이때 휴

대폰의 사용자는 메모리의 용량을 확장시키기 위하여 일정한 문자를 삭제하게 되는데 랜덤한 순서에 의하여 삭제되고 그 삭제된 부분은 0으로 채워지게 된다. 하지만 일부 업체의 휴대폰의 경우에는 플래시 메모리 부분에 메시지가 저장되고 SRAM 메모리 부분에서는 인터페이스 부분만 가지고 있다가 삭제되므로 플래시 부분에 저장되어 있는 메시지는 복원이 되기도 한다.

이때 스팸 메세지 또는 확인 후 저장하지 않고 바로 삭제되는 메시지는 일정한 메모리 공간을 차지하면서 헤더 글자만 보관하기도 하고 지속적으로 문자가 유입되는 경우에는 오래된 순서에 따라 문자가 삭제되는 것을 확인하였다.

이러한 FIFO(First In First Out)방식으로 삭제되는 정보는 문자 메시지뿐만 아니라 통화내역에 관한 정보로서 송신 통화내역, 수신통화내역, 부재중 통화내역등도 일정한 순서에 따라 삭제되므로 데이터가 유입되지 않았음을 확인 할 수 있었다.

V. 결 론

본 논문은 범죄의 압수수색 현장에서 간과하기 쉬운 전파의 유입으로 인하여 휴대폰의 기지국 서버에 저장되었던 정보가 휴대폰에 이동 저장되므로 수사에 필요한 기존의 디지털 증거가 무결성을 유지 하지 못해 법정의 증거 자료로 채택되지 못하는 문제점을 제시하였다[12].

이 문제점을 해결하기 위한 모바일 포렌식을 위한 이동통신 휴대폰의 압수수사 절차를 표준화하였고, 차단 봉투와 전파 차단실을 사용하여 압수된 휴대폰을 대상으로 통신을 시도하고, 인터넷 컴퓨터와 압수수색 휴대폰과의 네트워크상에서 연결을 하여 SMS를 사용한 무결성 훼손 실험을 하였다. 또한 압수수색 현장에서의 모바일 포렌식을 위한 무결성 훼손 사례를 실험하여 외국에서 사용하고 있는 전파 차단 봉투와 한국형 전파 차단 봉투를 사용하여 실험하였다.

실험 결과 압수한 당시의 휴대폰 자료와 실험 후의 휴대폰 자료가 일치함을 증명해 보임으로써 모바일 포렌식을 위한 무결성을 입증해 보였다.

향후 연구 되어야 할 과제로는, 모바일 포렌식을 위한 표준화된 분석과정과 분석도구, 그리고 전문가의 양성 등에 관하여 연구와 법 제도에 대한 연구기 필요하며, 새롭게 등장하는 첨단 분야 기술인 모바일 분야에 대한 제작사별 · 제품별 파일시스템 구조와 실무에서 문제가 되는 여러 가지 개인 프라이버시와 공권력의 절충 방안에 대한 법적 연구 등이 진행 되어야 할 것이다.

참 고 문 헌

〔1〕 정보통신부 통계자료, http://www.mic.go.kr/servlet/AutonomySearchServlet, *정보통신부*, 2007.7.

〔2〕 http://www.techsec.com/TF-2006-PDF/TF-2006-RickAyers-MobileForensics-TechnoForensics.pdf. p.3. 2007. 10.

〔3〕 이규안, 박대우, 신용태, "포렌식자료의 무결성 확보를 위한 수사현장의 연계관리 방법 연구". 한국컴퓨터정보학회 논문지, 제11권 제6호, pp.175-184, 2006. 12.

〔4〕 http://www.iemc.kr, *(주)EMC 네트워크*, 2007. 10.

〔5〕 Ing M.F. Breeuwsma, "Forensic Imaging of Embedded System Using JTAG (boandaryscan)", Digital Inverstigation 92006) 3 pp.33-42, 2006.

〔6〕 성진원, 백은주, 박창욱, 김역, 이상진, "휴대폰분석을 위한 도구 설계 및 구현" *한국디지털포렌식학회*, 디지털포렌식연구 창간호, pp.66, 2007.11.

〔7〕 디지털증거 처리 표준 가이드라인, *경찰청*, 2006. 12.

〔8〕 http://winnertechworld.com, *(주)워너텍월드*, 2007. 9. 6.

〔9〕 성진원, 백은주, 박창욱, 홍석희. "휴대폰 증거 데이터 분석을 위한 포렌식 도구" 제1회 안티포렌식 대응기술 워크샵, *고려대학교*, 2007.8.

〔10〕 김기환, 박대우. "모바일포렌식자료의 추출과 무결성 입증연구" *한국컴퓨터정보학회논문지*, 제12권6호, pp.181, 2007.12.

〔11〕 옥윤철, "휴대폰 알고보면 우습다" *도서출판 세화*, 2005. p.78.

〔12〕 Wayne Jansen, RickAyers "Guidelines on Cell Phone Forensics. *NIST*, 2007.

이 규 안 (Gyu-an Lee) 정회원

2006년 숭실대학교 정보과학대학원 정보통신학과 졸업
2008년 숭실대학교 컴퓨터학과 재학
2000년 벽성대학 정보통신 겸임교수
2002년 대검찰청 중앙수사부 근무
2005년 대검찰청 과학수사2담당관실 근무
2007년 대검찰청 디지털수사담당관실 근무
<관심분야> 유비쿼터스 보안, 디지털 포렌식, 해상 디지털 포렌식, 모바일 포렌식 · 보안

박 대 우 (Dae-woo Park) 정회원

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)
2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)
2000년 매직캐슬정보통신 연구소 소장, 부사장
2004년 숭실대학교 정보과학대학원 정보보안학과 겸임조교수
2006년 정보보호진흥원 선임연구원
2007년 호서대학교 벤처전문대학원 교수
<관심분야> 유비쿼터스 보안, 네트워크 보안 시스템, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality

신 용 태 (Young-tae Shin) 정회원

1985년 한양대학교 산업공학과 학사
1990년 Univ. of Iowa 전산학과 석사
1994년 Univ. of Iowa 전산학과 박사
1994년~1995년 Michigan State Univ. 전산학과 객원교수
1995년~현재 숭실대학교 컴퓨터학부 교수
<관심분야> 멀티캐스팅, 실시간통신, 이동통신, DRM 등