韓國 컴퓨터情報學會 論文誌
第12卷 第6號, 2007. 12.

2007-12-6-2-1

모바일 포렌식 자료의 추출과 무결성 입증 연구

김 기 환*, 박 대 우**

A Study on Extraction of Mobile Forensic Data and Integrity Proof

Ki-Hwan Kim*, Dea-Woo Park**

요 약

최근에는 IT기술의 발전으로 다양한 기능을 하는 모바일 정보 기기의 보급이 많이 늘어나고 있는 추세이다. 모바일 휴대폰을 이용하여 더 편리하고 효율적인 정보 교환 및 업무를 하는 순기능도 있지만, 휴대폰을 이용한 첨단기술자료 유출, 개인의 프라이버시 침해, 공갈 및 협박 등의 범죄의 수단으로 활용되는 역기능도 나타나게 되는 문제점들도 있다. 하지만 이러한 휴대폰을 이용한 범죄에 대해서는 법령 미비 등의 법적 연구도 부족할 뿐더러 수사 관점에서도 삭제, 복사, 이동이 쉬운 디지털증거의 특성상 객관적인 증거로 보장하기 위한 포렌식 디지털증거의 무결성을 입증하여야만 한다. 본 논문에서는 모바일 포렌식의 대표격인 휴대폰을 통하여 일어날 수 있는 디지털증거의 획득 방안에 대하여 실제 검증해보고 해시함수를 이용하여 디지털증거의 무결성을 입증하는 방안을 연구하는데 목적이 있다.

Abstract

Lately, it is a trend that diffusion of Mobile Information Appliance that do various function by development of IT technology. There is function that do more convenient and efficient exchange information and business using mobile phone that is Mobile Information Appliance, but disfunction that is utilized by pointed end engineering data leakage, individual's privacy infringement, threat, etc. relationship means to use mobile phone is appeared and problems were appeared much. However, legal research of statute unpreparedness and so on need research and effort to prove delete, copy, integrity of digital evidence that transfer secures special quality of easy digital evidence to objective evidence in investigation vantage point is lacking about crime who use this portable phone. It is known that this Digital Forensic field is Mobile Forensic. In this paper, We are verify about acquisition way of digital evidence that can happen in this treatise through mobile phone that is Mobile Forensic's representative standing and present way to prove integrity of digital evidence using Hash Function.

▸ Keyword : forensic, hash function, mobile forensic, ubiquitous security

• 제1저자 : 김기환, 교신저자 : 박대우(prof1@paran.com)
• 접수일 : 2007.9.11, 심사일 : 2007.10.31, 심사완료일 : 2007.11.9.
* STG Security, ** 호서대학교 벤처전문대학원 교수

Ⅰ. 서 론

IT 정보기술의 발달로 컴퓨터의 이용이 생활화 되어 가고 있다. 더욱이 컴퓨터가 소형화, 다양화되어 기존의 고정되고 무거운 컴퓨터가 아닌 이동성과 휴대성을 지원하는 모바일 정보기기의 사용이 크게 늘어나고 있다. 특히, 컴퓨터가 책상위의 데스크 탑 을 벗어나서 휴대하기 편한 노트북, PDA 등이 나왔으며, 최근에는 음성통화 기능뿐만 아니라 VoIP, MP3, 디지털카메라, DMB, 게임기, 내비게이션 기능 등 다양한 기능을 하는 모바일 기기의 보급이 많이 늘어나고 있는 추세이다[1]. IT기술을 통한 장비의 발전으로 시간과 장소에 구애 없이 언제어디서든 인터넷을 통하여 일반 데이터 자료뿐만 아니라 영상까지도 주고받는 유비쿼터스 (Ubiquitous) 컴퓨터 네트워크 환경에서 살아가고 있는 것이다.

또한 모바일 기기는 점점 더 소형화되고 다양한 기능을 갖게 되어 모바일기기의 대표 격인 휴대폰은 기존 통화기능에서 벗어나, WiBro를 이용한 휴대인터넷에서의 업무 처리를 하며, 음악을 들으며 여가 활동을 할 수 있는 MP3기능, 사진 및 동영상을 찍어 사진 자료를 즉시로 보내거나 저장하며, 선명한 화질의 뉴스 및 영상 시청이 가능한 DMB 기능, GPS를 통한 경로설정이 가능한 내비게이션 기능, 서로의 회상통신까지 가능한 3세대의 휴대폰들이 보급되고 있는 실정이다. 즉, 실제 생활과 업무에서 휴대폰을 통하여 PC에서 하던 업무뿐만 아니라 이동성의 장점을 가진 즉시적 현장 업무를 휴대폰을 통하여 업무를 실시간으로 처리 할 수 있는 유비쿼터스 세상이 된 것이다.

이러한 모바일 기기를 이용하여 더 편리하고 효율적인 생활 및 업무를 하는 순기능도 있지만, 모바일 기기와 디지털카메라를 이용한 첨단기술자료 유출, WiBro의 휴대인터넷을 이용한 불법적인 해킹[2]과 불법적인 금융거래, 개인의 프라이버시 침해, MP3, 모바일 컨텐츠의 불법적인사용, VoIP 연결을 통한 도청[3]과 사기의 범죄의 수단으로 활용되기도 하고 모바일뱅킹을 해킹하여 금융사고 및 네트워크 시스템 마비를 일으키는 Dos, DDoS 공격[4] 등의 역기능을 가진 문제점들을 발생하게 된다.

하지만 이러한 모바일 기기를 이용한 범죄에 대해서는 법령미비 등의 법적 연구도 부족할뿐더러 수사 관점에서도 삭제, 복사, 이동이 쉬운 디지털증거의 특성상 객관적인 증거로 보장하기 위한 디지털증거의 무결성(integrity)[5]을 입증하기 위한 연구와 노력이 필요하게 되었다. 이러한 디지털 증거는 모바일 컴퓨터 범죄의 증거라고 볼 수 있으며 디지털 증거의 수집 및 분석 그리고 법정에 제출하는 과정의 일관된 연계성과 무결성을 입증하는 것이 중요하다고 할 수 있다.

최근 유비쿼터스 환경에서 사용되는 모바일기기들은 급속한 발전 및 보급이 확대 되면서 컴퓨터 관련 범죄뿐만 아니라 일반 범죄에서도 중요 증거 또는 단서를 모바일 기기의 저장장치 속에 보존되고 있거나 삭제된 데이터에 대한 압수 수색 등 디지털증거의 습득 ·복원하는 일련의 과정 속에서 무결성을 입증하는 방안이 필요하게 되었다. 특히 모바일 기기의 대표라 할 수 있는 휴대폰에서의 디지털증거 수집, 증거 분석, 증거에 대한 무결성 증명 등이 필요가 많아지고 있는 상황이지만, 국내의 CDMA(Code Division Multiple Access) 휴대폰에 대한 모바일 포렌식 도구가 전무한 것이 현실이다.

본 논문에서는 휴대폰에서의 디지털 증거의 추출 방안 및 실험을 통한 검증 및 해시 함수를 이용한 모바일 포렌식 자료에 대한 증거의 무결성을 입증을 할 수 있는 방안에 대하여 고찰 하려고 한다.

또한 모바일 기기들의 대표 격인 휴대폰에서 디지털 증거의 획득 방안에 대하여 실제 검증해보고 이러한 휴대폰의 디지털증거의 무결성을 입증하는 방안을 연구하고, 제시 하는데 목적이 있다.

Ⅱ. 관련 연구

2.1. 모바일 포렌식

2.1.1. 모바일 포렌식 의미

모바일 포렌식은 디지털 포렌식[6]의 일종으로 휴대폰, 노트북, PMP, PDA 등의 모바일기기와 이동장치인 차량, 선박, 기차, 비행기 등에 장착된 블랙박스와 같은 이동장치를 대상으로 하여 범죄나 수사에서 디지털 증거를 수집, 식별, 추출, 보존, 문서화하여 법정에 제출하는 일련의 행위를 말한다. 외국의 경우에는 'Mobile Forensics'라는 명칭을 사용하거나 각각의 대상에 따라 'Mobile Phone Forensics' 또는 'Cell Phone Forensics', 'PDA Forensics'등의 세부적인 명칭을 함께 사용하고 있기도 하다.

2.1.2. 모바일 기기와 모바일 포렌식의 특징

가. 모바일 기기(휴대폰)의 특징

모바일 정보 기기는 휴대폰, 노트북, PDA, MP3, 카메라, PMP 등의 휴대 가능한 모든 디지털 정보 기기와 이동장치인 차량, 선박, 기차, 비행기 등에 장착된 블랙박스와 같은 이동

장치를 말한다. 그 중에 대표적인 모바일 기기인 휴대폰은 기기의 컨버전스(Convergence)로 다양한 기능들이 통합되고 있는데, 휴대폰의 경우에는 PDA, MP3, 카메라, 내비게이션, PMP 기능 등이 추가 되고 있는 상황 이다. 그래서 휴대폰은 음성 통신뿐만 아니라, 인터넷 접속을 하여 컨텐츠 조회를 통한 교통의 흐름, 증권 정보, 음성 사서함 등의 데이터 송수신도 가능하고 사진 촬영, 동영상 촬영, MP3, DMB에서 TV 수신까지도 가능하여 범죄에 이용되고 있다.

나. 모바일 기기(휴대폰)의 하드웨어

휴대폰은 하드웨어적으로 컴퓨터와 같이 기본적인 중앙처리장치인 CPU, 데이터 저장을 위한 저장장치, 데이터 입출력을 위한 입출력 장치 등을 가지고 있다. 즉, 마이크로프로세서, ROM, RAM, 무선모듈, 디지털 신호 프로세서, 마이크로폰과 스피커, 하드웨어 키와 다양한 인터페이스와 LCD를 가지고 있다[7].

표 1은 휴대폰의 구분에 따른 하드웨어의 특징을 나타내고 있다. 최근의 휴대폰들은 멀티 사용이 가능한 고성능의 마이크로프로세서가 탑재되어 나오며, 내장 메모리도 1GB정도의 큰 메모리 용량의 신제품 들이 많이 나오고 있다. 또한, MiniSD, MMC mobile 들이 지원되는 외장 메모리 슬롯이 장착 되어 있으며, 입력장치로는 기존의 키패드 외에 터치스크린, 카메라가 장착된 모델이 나오고 있다. 또한 장거리 통신에서는 GSM, CDMA와 더불어 HSDPA, HSUPA, 단거리 통신에서는 적외선통신(IrDA) 또는 블루투스 같은 무선통신은 휴대폰에 내장되어 있다.

표 1. 휴대폰에서의 하드웨어 특징 비교
Table 1. Hardware Characteristic comparison in Mobile Phone

구 분	휴대폰	스마트폰/PDA폰
OS	휴대폰 전용OS탑재	휴대폰용OS+PDA (WinCE,Plam) 동시탑재
CPU	1 CPU(Phone)	2 CPU(Phone/PDA)
메모리	주로 내장 메모리	내장 메모리 + 외장 메모리 (Mini SD)
입력장치	Keypad, CCD	Touch screen, Keypad, CCD

휴대폰의 OS는 특정 도구를 사용하여 전자적으로 지우고 다시 프로그래밍 할 수 있는 ROM에 저장하는데, RAM의 경우 배터리가 있을 때만 데이터가 유지되고, 배터리가 나가거나 배터리를 다 쓴 경우에는 데이터를 잃게 된다.

다. 모바일 기기(휴대폰)의 모바일 포렌식 자료 획득

휴대폰에서 범죄와 관련된 증거를 획득하기 위해서는 우선, 휴대폰의 저장 장치로 쓰이고 있는 플래시 메모리에서 데이터를 추출해야한다. 휴대폰에서 사용하는 플래시 메모리는 형태에 따라서 외장메모리와 내장 메모리의 2가지로 나눌 수 있다.

외장형 플래시 메모리에서 데이터를 추출하는 경우에는 회사별로 규격과 특성이 다르므로 그에 맞는 드라이버와 인터페이스를 준비 하여야 한다. 단 외부적으로 연결하여 사용하는 경우에는 기기의 특성상 인터페이스 연결에 문제가 되어 실제 데이터는 복구 되지 않는 경우가 발생할 수 있으므로 메모리 저장장치를 다룸에 있어서는 상당한 주의를 요한다.

USB 메모리 멀티 인터페이스장치를 이용하여 연결하고, 플래시 메모리에 쓰기 방지장치가 되어 있는 경우에는 쓰기방지장치를 이용하여 디지털증거의 정보를 미러링 방식을 사용하여 복제본을 만든 다음 복원 및 데이터 검색을 하게 된다. 이때 쓰기방지 장치가 되어 있지 않다면, 디지털 증거의 무결성을 입증하기 위하여 플래시 메모리 쓰기 방지장치를 별도로 연결한 다음 데이터를 추출 하도록 한다. 이렇게 하여 추출된 데이터는 일반적으로 컴퓨터 포렌식[8]에서 많이 쓰이고 있는 Encase 라는 컴퓨터 포렌식 분석 툴을 사용하여 데이터의 수집 및 복원과 분석을 할 수 있다.

이러한 특성 때문에 현재 모바일 기기의 전반에 걸쳐 플래시 메모리의 저장능력은 1GB이상으로 급속하게 증가하고 있으며, 플래시 메모리에 저장된 디지털정보의 추출 및 복원을 위하여 많은 연구를 하고 있다.

2.1.3. 모바일 포렌식 분석 도구

가. 모바일 포렌식 분석 도구

포렌식 분석도구의 종류중의 하나인 모바일 포렌식 분석도구는 모바일 정보기기의 대표 격이라 할 수 있는 휴대폰을 대상으로 하는 포렌식 분석도구이다. 하지만, 표준화되어있는 컴퓨터 포렌식 분석도구와는 달리 모바일 포렌식 분석도구의 대상인 휴대폰은 각 제조사별로 운영체제가 틀린 관계로 생산되어 있는 전체 휴대폰에 대한 분석이 힘든 것이 현실이다.

더욱이 휴대폰이 제조되어 폐기되는 생명주기가 매우 짧기 때문에 모바일 포렌식 분석도구를 개발하는 담당자들은 새로운 휴대폰이 나오자마자 대응해서 휴대폰에 맞는 분석도구를 개발하고, 휴대폰의 변화에 따라서 계속적으로 지원을 하기 위하여 모바일 포렌식 분석도구를 업그레이드해야 한다.

모바일 포렌식 분석도구는 휴대폰의 저장장치인 플래시 메모리에서 디지털증거를 획득하기 위해서는 다음의 2가지 방

법으로 접근해야 한다. 첫째, 물리적인 방법으로서 플래시 메모리에 있는 데이터를 bit-by-bit로 전체 데이터를 복사한다. 둘째, 논리적인 방법으로서 파일시스템의 파티션처럼 논리적인 저장 공간에 저장되어 있는 파일이나 디렉토리 같은 데이터를 휴대폰으로부터 컴퓨터로 복사하는 것을 의미한다. 이때 대부분의 포렌식 분석 도구들은 휴대폰 과 컴퓨터간의 동기화하고 통신하기 위하여 일반적인 휴대폰의 드라이버를 먼저 설치하여 데이터를 추출하게 된다.

나. 모바일 포렌식 분석 도구의 비교

표 2. 모바일 포렌식 분석도구의 비교(9)
Table 2. Comparison of a Mobile Forensic Analysis Tool

Promised Results	Tools				
		TULP 2G	OPM	MOBILedit!	Cell Seizure
	MD5	Unknown	Unknown	Not Found	Yes – Unreliable
	SHA1	Unknown	Unknown	NA	Not Found
	Reports - HTML	NA	Unknown	NA	Yes
	Reports – XLS	Unknown	Unknown	Yes	NA
	Reports – XSL	NA	NA	Yes	NA
	Reports – CSV	NA	Unknown	NA	NA
	Reports – XML	NA	NA	Yes	NA
	Reports – RTF	NA	Unknown	Yes	NA
	Reports - TXT	Unknown	Unknown	Yes	Yes
	Compatibility with Windows	XP, unknown others	2000, unknown others	2000, unknown others	2000, unknown others
	GSM	Unknown	Yes	Yes	Yes
	CDMA	Unknown	Yes	Beta Support	Incompatible with 6385
	Backup	Unknown	Unknown	Yes	Yes

모바일 포렌식 분석 도구의 종류는 대상 휴대폰의 종류에 따라서 크게 2가지로 나눌 수가 있는데, 첫째, 국내에서 많이 쓰이는 CDMA방식의 휴대폰을 대상으로 하는 분석도구와 외국에서 많이 쓰이는 GSM방식의 휴대폰을 대상으로 하는 분석도구로 나눌 수 있다.

표 2와 같이 모바일 포렌식 분석 도구는 지원하는 대상 인 휴대폰과 데이터 추출 방법 등에서 차이를 보이고 있다.

모바일 포렌식 분석 도구는 CDMA 휴대폰의 경우에는 플래시 내장, 외장 메모리에서 데이터를 추출하며, GSM 휴대폰의 경우에는 GSM의 SIM카드같이 외장형 식별 모듈에서 데이터를 추출하기 위하여 설계되었다. 모바일 포렌식 분석 도구와 비 포렌식 도구는 대상 휴대폰과 동기화 및 통신을 하기 위하여 같은 드라이버를 을 사용하기도 하지만 정식 포렌식 분석 도구는 대상 휴대폰에서 데이터를 추출하기만 하고 데이터를 쓰거나 수정하지는 못하도록 설계된 반면에 비 포렌식 분석도구는 대상 휴대폰에서 데이터를 읽고 쓰고 수정하는 것이 모두 가능하므로, 비 포렌식 분석도구를 사용하여 디지털증거를 획득 시에는 원본데이터의 손상 및 훼손이 되지 않도록 유의하여 디지털 증거의 무결성이 문제가 되지 않도록 해야 한다(10).

2.1.4. 디지털 증거 추출 도구

모바일 포렌식 도구가 없는 상태에서 휴대폰의 디지털 증거를 획득하기 위해서는 휴대폰 제조사에서 제공하는 데이터 추출 도구를 활용할 수가 있다. 휴대폰의 플래시 내장 메모리에 있는 데이터를 추출하기 위해서는 분석 대상 휴대폰의 모델에 따라 적당한 방법을 선택해야 한다.

본 논문에서는 표 3에 나와 있는 증거 추출 도구 중에서 퀄컴사에서 휴대폰 제조업체에 무상으로 제공하는 QPST(Qualcomm Phone Service Tool)라는 프로그램을 실험에 사용하였다. 이 프로그램을 이용하여 휴대폰의 걸어놓은 비밀번호를 알아내고, 휴대폰의 플래시 내장 메모리에 있는 SMS, 스케줄, 메모 등의 원시 데이터를 추출할 수 있었다.

표 3. 디지털 증거 추출 도구의 비교
Table 3. Comparison of a Digital Evidence Abstraction Tools

분석도구	소 개	기 능	쓰기 방지	안정성
QPST	휴대폰제조업체인 퀄컴사에서 무료로 제공하는 휴대폰 개발 툴(Tool)	- 휴대폰내장메모리의 파일시스템뷰어 - 휴대폰데이터의 추출 및 삽입 기능	없음	불안정
EasyCDMA	Pinksoft사에서만든 휴대폰을 PC에 연결하는 툴(Tool)	- 휴대폰내장메모리의 파일시스템뷰어 - 휴대폰데이터의 추출 및 삽입 기능	없음	안정적
Bitpim	GNU 일반 공중 사용 허가서에 적용받는 Open Source프로그램으로 휴대폰의 포렌식분석을 위한 툴(Tool)	- 휴대폰내장메모리의 파일시스템뷰어 - 휴대폰데이터의 추출 및 삽입 기능 - GSM폰 포렌식 분석 기능	있음	매우 안정적
비고	분석상한계 : -정상 파일만 분석(삭제 된 파일은 분석 불가) -데이터가 생성, 삭제, 수정된 시간을 알기 어렵다.			

2.2. 모바일 포렌식의 현황과 문제점

표 4와 같이 모바일 포렌식은 컴퓨터 포렌식에 비해서 몇 가지 문제점을 가지고 있어 최근에 영국이나 미국에서 연구가 진행되고 있다. 영국의 휴대폰 방식은 GSM방식을 , 미국은 GSM방식과 CDMA방식을 모두 사용하고 있으며, 각각에 맞는 방식으로 모바일 포렌식 의 지침, 모바일 포렌식의 분석 도구 등을 개발 하여 사용하는 등 모바일 포렌식에 대한 연구가 체계적으로 진행되고 있다.

반면 국내에서의 모바일 포렌식 연구는 아직 초기 단계를 벗어나지 못하고 있으며, 모바일 포렌식 분석도구의 개발도

전무한 상태이다. 또한 외국의 모바일 포렌식 분석도구는 퀄컴 칩을 사용하는 국내의 CDMA휴대폰 방식과 상이하고 휴대폰 모델별 운영체제 및 플래시 메모리의 파일 시스템이 달라 사용하는데 몇 가지의 한계가 있다.

표 4. 컴퓨터 포렌식과 모바일 포렌식의 문제점 비교
Table 4. Problem comparison of Computer Forensic and Mobile Forensic

구 분	컴퓨터 포렌식	모바일 포렌식
대상	컴퓨터의 하드디스크	휴대폰의 플래시 메모리
파일시스템	표준화 (NTFS, FAT)	비표준화 (제조사별 고유의 운영체제)
운영 체제	표준화 (Windows, Linux)	비표준화 (제조사별 고유의 운영체제)
분석 도구	EnCASE, DIES 등	국내 CDMA용 분석도구 없음
life Cycle	비교적 길다.	매우 짧다.

그래서 휴대폰에서 디지털증거를 획득하려면 휴대폰 제조업체에서 제공하는 소프트웨어를 사용하여 분석 할 수밖에 없는 상황이다[11].

2.3. 해시 함수 알고리즘

2.3.1. 해시 함수 알고리즘

해시 함수 알고리즘은 크게 DES와 같은 블록암호알고리즘에 기초한 해시 알고리즘과 전용 해시 알고리즘으로 나눌 수 있다. 블록암호를 이용한 해시 알고리즘은 이미 구현되어 사용되고 있는 블록암호를 사용할 수 있다는 이점이 있으나, 대부분의 불록암호 알고리즘의 속도가 그리 빠르지 않을뿐더러 이를 기본함수로 이용한 해시 알고리즘의 경우 블록암호보다도 훨씬 더 속도가 떨어지므로 현재는 대부분의 응용에서 전용 해시 알고리즘이 주로 이용된다.

해시 함수인 MD5 알고리즘은 데이터 무결성 및 메시지 인증 등에서 사용할 수 있는 함수로써 정보보호의 여러 메커니즘에서 이용되는 핵심 요소기술이며, 최근에는 디지털 증거의 무결성 입증에 활용되고 있는 알고리즘이다. 해시 알고리즘이란 임의의 길이의 비트 열을 고정된 길이의 출력 값인 해시코드로 압축시키는 함수이며, 암호학적 응용에 사용되는 대부분의 해시 함수는 강한 충돌저항성을 지닐 것이 요구된다. 암호학적 해시 알고리즘의 충돌 저항성은 디지털 서명에서 송신자외의 제 3자에 의한 문서위조를 방지하는 부인방지 서비스를 제공하기 위한 필수적인 요구조건이 된다.

2.3.2. 해시 함수 기술과 전자서명

해시 함수는 임의의 입력 비트열에 대하여 일정한 길이의 안전한 출력 비트열을 내는 것으로, 정보통신 보호의 여러 메커니즘에서 활발히 이용되는 요소 기술이다.

해시 함수란 입력 데이터 스트링을 고정된 길이의 출력인 해시코드로 대응시키는 함수로서 첫째, 주어진 해시코드에 대하여 해시코드를 생성하는 데이터 스트링을 찾아내는 것은 불가능하며, 둘째 주어진 데이터 스트링에 대하여 같은 해시코드를 생성하는 또 다른 데이터 스트링을 찾아내는 것은 불가능하다는 두 가지 성질을 만족하는 함수를 말한다. 여기서 계산상의 실행 가능성의 여부는 사용자의 특정한 보안 요구와 환경에 영향을 받는다.

해시 함수는 전자서명에 많이 사용되고 있다. 입력 M 해시 함수를 취한 결과인 해시코드 h(M)에 송신자는 비밀키로 서명을 하고, 수신자는 공개키로 확인한 후, 그 결과 h(M)을 수신된 M에 해시 함수를 취한 결과의 값과 비교하여 서명의 진위 여부를 밝힌다.

따라서 해시 함수는 정보의 무결성 증명에 활용 될 수 있다. 무결성 검증을 원하는 정보의 해시코드를 계산하여 안전하게 보관하다가 무결성 검증이 필요할 때 다시 해시코드를 계산하여 보관한 해시코드의 값과 비교함으로써 정보의 무결성을 확인할 수 있다[12].

III. 휴대폰에서 모바일 포렌식 증거 획득 방안

3.1. 휴대폰에서의 모바일 포렌식 실험

국내의 휴대폰은 퀄컴사의 칩을 사용하며 기본적으로 SMS 메시지, 스케줄, 메모 등의 데이터를 휴대폰 단말기의 플래시 내장 메모리 가지고 있다. 하지만, 제대로 된 모바일 포렌식 도구가 없는 상태에서 휴대폰 제조사의 툴만을 가지고도 휴대폰에서의 디지털 증거의 추출이 가능한지 다음과 같이 실험을 해보았다.

3.1.1. 모바일 포렌식을 위한 실험 환경

휴대폰에서의 디지털 증거를 추출하기 위한 실험 환경은 표 5와 같다.

표 5. 휴대폰의 모바일 포렌식 증거 추출 테스트 환경
Table 5. Mobile Forensic evidence abstraction test environment of Mobile Phone

항 목	사 양
PC	CPU : Pentium IV Memory: 512MB OS : Windows XP HDD : 160GB
휴대폰	명 칭 : KTF-X3500 통신사 : KTF 제조사 : (주)KTF Tech
Cable	명 칭 : USB케이블
추출 도구	명 칭 : QPST. 제조사 : Qualcom
에디터	명 칭 : UltraEditor 제조사 : IDM

3.1.2. 모바일 포렌식을 위한 데이터 추출 단계

휴대폰에서 증거는 단말기의 내장 메모리에서 데이터를 추출하는 단계이다. 모바일 포렌식 증거를 추출하여 분석하는 과정에서 증거물이 훼손되거나 수정될 경우 증거물의 가치를 상실할 수 있으므로 항상 주의해야 한다. 모바일 포렌식 증거를 추출하는 과정은 다음과 같다.

가. 휴대폰 과 PC의 연결

그림 1과 같이 휴대폰 USB 케이블을 이용하여 PC의 USB 포트에 접속하고, 휴대폰의 USB 단자에 연결한 다음 휴대폰 제공업체에서 제공하는 USB 드라이버를 설치한다.

그림 1. 휴대폰과 PC의 연결
Fig. 1. Connection of Mobile Phone connect to PC

나. 모바일 포렌식 증거 분석을 위한 툴 설치

휴대폰에서 모바일 포렌식 증거를 추출하기 위해서는 휴대폰 분석 툴을 결정해야 한다.

본 논문에서는 QPST[13], EasyCDMA, Bitpim 중에서 퀄컴사의 QPST를 이용하여 휴대폰에서 디지털증거를 추출하도록 한다.

QPST 툴은 휴대폰의 분석 툴이므로, 본 논문의 연구를 위해 휴대폰의 증거 추출 과정에서는 데이터의 무결성을 고려하지 않고 테스트를 하였다.

다. 휴대폰 암호 확인

휴대폰에 암호가 설정되어 있을 경우에는 내장 메모리에 있는 SMS, 사진, 기타 데이터를 휴대폰 제조사에서 제공하는 소프트웨어로도 디지털 증거의 추출이 힘들다. 이럴 경우에도 그림 2와 같이 QPST를 이용하여 휴대폰의 암호를 알아낼 수 있어서 휴대폰에서의 디지털 증거의 추출이 가능하다.

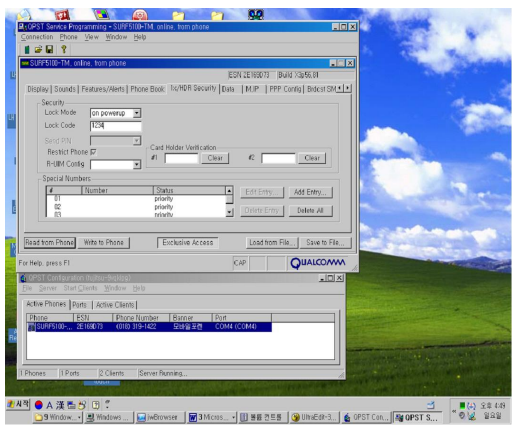

그림 2. QPST를 이용하여 휴대폰 암호 알아내기
Fig. 2. Find out Mobile Phone password using QPST

3.1.3. 모바일 포렌식 증거 자료 추출

본 논문의 3.1.2. 다에서 휴대폰의 암호를 알아 낸 경우, 휴대폰 제조사의 툴을 이용하여 그림 3과 같이 기본적인 사진, 주소록 등의 자료의 추출이 가능하다.

그러나 휴대폰 제조사에서 정한 기본적인 데이터 이외의 자료는 추출이 불가능 하므로 QPST를 이용하여 대상 휴대폰의 내장 메모리의 디지털 증거들을 추출 하도록 한다.

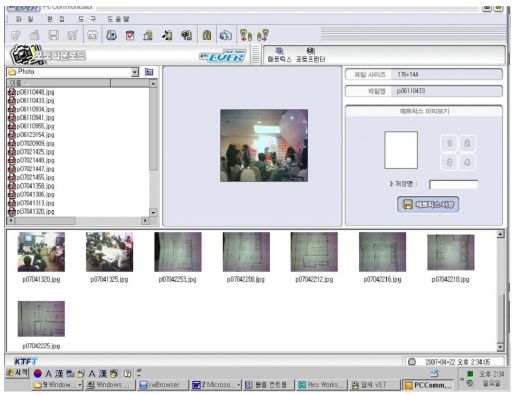

그림 3. 휴대폰 제조사의 툴을 이용한 디지털 증거(사진) 추출
Fig. 3. Digital evidence(picture) abstraction that use tool of Mobile Phone Manufacturer

가. 휴대폰 분석 툴을 활용한 증거 자료 추출

휴대폰 제조사에서 제공하는 툴을 활용하여 기본적인 디지털증거 뿐만 아니라 내장 메모리에 있는 파일을 직접 추출 해 내기 위하여 휴대폰 분석 툴인 QPST를 실행하면 그림 4와 같이 내장 메모리의 루트 디렉토리의 자료를 확인할 수 있다.

디렉토리 별로 사진, SMS의 파일들이 있으며 이중에서 SMS에 해당되는 파일을 PC로 복사한다.

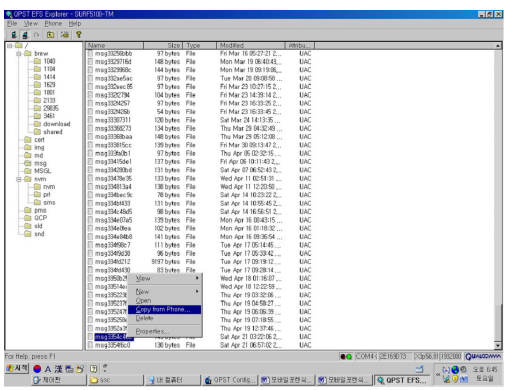

그림 4. 휴대폰 제조사의 툴을 이용한 디지털 증거(SMS) 추출
Fig. 4. Digital evidence (SMS) abstraction that use tool of Mobile Phone Manufacturer

나. 휴대폰 분석 툴을 활용한 모바일 포렌식 증거 분석

휴대폰에서 추출한 디지털증거 파일은 일반 텍스트 파일이 아닌 관계로 일반 워드에서는 확인 할 수가 없었다. 그래서 그림 5와 같이 헥사코드 분석 툴인 Ultra Editor를 통하여 휴대폰에서 추출된 SMS 메시지 의 내용, 발신자 전화번호 및 시간의 정보 확인이 가능 하였다.

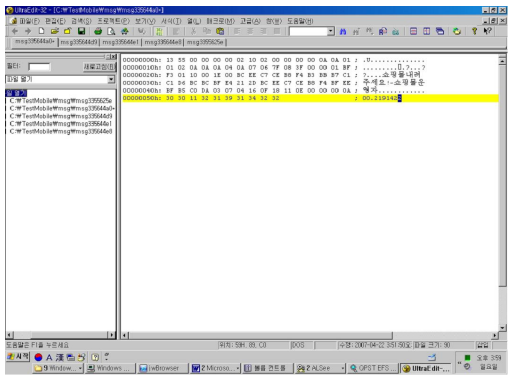

그림 5. Ultra Editor를 이용한 디지털 증거(SMS) 분석
Fig. 5. Digital evidence(SMS) analysis that use Ultra Editor

3.2. 휴대폰에서의 모바일 포렌식 증거의 문제점

3.2.1. 모바일 포렌식 증거의 추출 및 분석 시 문제점

가. 휴대폰 회사별 신제품에 따른 포렌식 툴 부재

상당히 많은 종류의 휴대폰 신제품이 계속 판매되고 있다. 이 경우 각 제조사별, 모델별 휴대폰이 운영체제 및 표준화가 되어 있지 않아서, 휴대폰의 디지털증거를 추출 및 분석하여 증거화 할 수 있는 모바일 포렌식 도구의 개발이 힘든 환경이다.

나. 휴대폰 회사별 신제품의 내부 구조 차이

휴대폰의 저장매체인 내장 메모리의 구조 및 저장위치가 제조사별, 모델별로 틀리고, 개발 모델에 따른 내부 구조는 각각 회사의 기술 개발에 대한 기밀 사항이므로 내부 구종의 차이에 따른 모바일 포렌식 추출 및 분석이 어렵다.

다. 휴대폰의 수명이 짧다.

휴대폰 제조회사는 지속적인 신제품의 창출로 새로운 휴대폰을 개발하여 상용화하고 있고, 또한 유행이나, 기능, 디자인, 마케팅(Marketing), 가격의 변동에 차별화된 휴대폰이 있다. 결국 이 다양한 휴대폰 모델 별로 적절히 연결되는 모바일 포렌식 도구 개발 및 업데이트가 힘든 환경이다.

3.2.2. 모바일 포렌식의 무결성 문제점

첫째, 내장된 플래시메모리에서 삭제된 데이터를 복원 할 수 있는 기법 및 툴이 없는 상황이다.

둘째, 휴대폰에서의 디지털 증거에 대한 신뢰성을 확보하여 법정증거로서의 역할을 하기위해서는 디지털증거의 무결성 확보가 중요한 요소이다.

그러나 현재 국내에는 휴대폰의 디지털증거에 대하여 디지털증거 추출, 분석, 무결성 증명에 필요한 모바일 포렌식 툴이 거의 없는 상황이어서 법정 증거로 채택되기 위해서는 별도의 절차 및 검증 기술에 대한 연구가 필요하다.

Ⅳ. 모바일 포렌식 무결성 입증 방안

4.1. 해시함수를 이용한 무결성 입증 방안

모바일 기기에서 디지털 증거를 획득하거나 분석하는 과정에서 원본데이터의 변형이나 훼손이 발생해서는 않된다. 디지털 증거를 분석하기 전에 무결성을 유지하기 위하여 미러링 방식으로 복사본을 만들고, 무결성 입증을 위해 해시 함수를 이용하여 파일별로 비교 후 무결성을 입증 할 수 있다[14].

4.2. 해시함수를 이용한 무결성 입증 과정

그림 6에서 휴대폰에서 최초로 추출한 디지털 증거 파일 A를 해시 함수를 통한 해시값과 캐릭터 한 개만이라도 변조한 디지털 증거 사본 파일 B를 해시 함수로 하였을 때 해시값은 완전히 다르게 나오므로, 해시 함수를 이용 해시값을 비교하면 디지털 증거가 원본의 데이터 파일인지의 여부 즉, 디지털증거의 무결성을 검증할 수 있는 결과 값을 검증 할 수 있다[15].

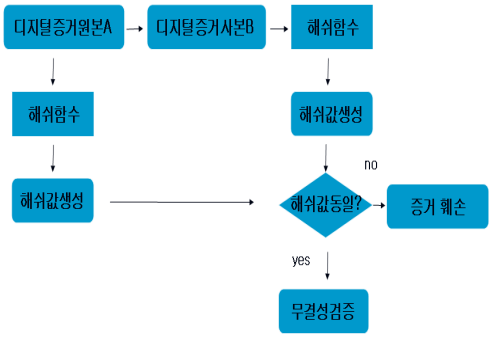

그림 6. 해시 함수를 이용한 무결성 검증
Fig. 6. Integrity verification that use Hash function

즉, 해시값 a = a′ 일 때는, 디지털 증거의 내용이 변조되지 않음이 보장된다. 반면, a ≠ b 일 때는, 디지털 증거의 내용이 변조되었음을 뜻한다. 일방향 함수인 해시 함수의 결과 값을 비교하여 값이 같다면, 디지털 내용의 무결성 을 입증 할 수 있는 것이다.

4.3. 휴대폰 압수 후 무결성 입증 과정

범죄의 현장에서 최초 핸드폰을 압수할 당시에, 압수 시간에 대한 다른 휴대폰과의 동일 시간에 대한 사진을 찍어 증거자료를 남기고, 즉시 전원을 끈 상태에서 전파 차단 봉투 속에 밀봉하여 휴대폰의 일차 무결성을 확보하고, 수사 본부에 가져온 휴대폰은 전파차단실 내에서 휴대폰에서 추출된 디지털 증거에 대하여 해시 함수를 설정해 놓아, 향후 모바일 포렌식 증거 자료에 대한 이차 무결성 을 증명 할 수 있다.

즉, 휴대폰의 압수 후에 임의의 조작이나 변조를 할 경우에는 무결성을 검증하기 위한 해시 함수 값이 달라지기 때문에, 범죄에 사용된 휴대폰의 모바일 포렌식 자료에 조작을 했다는 증거가 된다.

따라서 법정에 자료 제출 전에 해시 함수 값의 일치성에 대한 검증과정을 실시하여, 증거자료로 첨부하면 모바일 포렌식에서 법정 범죄 증거자료에 대한 무결성을 입증 할 수 있다.

Ⅴ. 결론

본 논문에서는 모바일 기기 중에 대표적으로 가장 많이 쓰이고 있는 휴대폰에서 증거가 저장되는 플래시 메모리의 저장 구조를 통하여 포렌식 증거의 획득하는 방안 및 분석 하는 과정뿐만 아니라, 별도의 해시 함수를 이용한 모바일 포렌식 증거의 무결성 입증 방안을 연구해 보았다.

휴대폰에서 모바일 포렌식 증거 획득 방안으로 QPST QPST 툴을 PC에 설치하고, 휴대폰에 USB 케이블로 연결되어 휴대폰에서 추출된 SMS 메시지의 내용, 발신자 전화번호 및 일시의 확인을 헥사코드 분석 툴인 Ultra Editor를 통하여 증거 자료의 확인이 가능 하였다.

또한 모바일 기기에서 디지털증거를 획득하거나 분석하는 과정에서 원본 데이터의 변형이나 훼손이 발생해서는 않되므로, 모바일 포렌식 증거의 무결성 입증 방안을 연구하였다.

본 논문에서는 범죄의 현장에서 최초 핸드폰을 압수할 당시에, 압수 시간에 대한 다른 휴대폰과의 동일 시간에 대한 사진을 찍고, 즉시 전원을 끈 상태에서 전파 차단 봉투 속에 밀봉하여 휴대폰의 일차 무결성을 확보하고, 본부에 가져온 휴대폰은 전파차단실 내에서 미러링 방식으로 휴대폰 자료에 대한 복사본을 만들고, 다음에 디지털 증거에 대하여 해시 함수를 설정해 놓아 모바일 포렌식 증거 자료에 대한 법정에 제출 전에 파일별로 해시 값을 비교하여 모바일 포렌식 자료의 무결성을 입증 할 수 있다.

본 논문에서 연구된 휴대폰에서의 모바일 포렌식은 범죄나, 민사 형사상의 증거 자료로서의 역할 때문에 앞으로 더욱

더 많은 필요성이 대두될 것이다.

향후 연구로는 휴대폰의 DMB, 전자인증 기능과 VoIP 및 휴대 영상전화를 통한 범죄가 점차 늘어나고 있는 추세이므로 휴대폰에서의 각각의 기능별로 모바일 포렌식 증거의 무결성을 입증하는 방안과, 휴대폰과 이동 기기 등의 블랙박스 등의 기종에 상관없이 적용이 가능한 증거 획득 및 분석, 검색, 보고서가 가능한 한 종합 모바일 포렌식 도구의 연구 개발 및 검증과 법과 제도에 관한 연구가 이루어져야 하겠다.

참고문헌

〔1〕 신용태 외, "모바일 DRM 기술 분석 및 시장 동향'. 정보과학회지, 제23권 제8호, 2005. 9.

〔2〕 박대우, 임승린. "WiBro에서 공격 이동단말에 대한 역추적기법 연구." 한국컴퓨터정보학회논문지, 제12권 제3호, 2007. 7.

〔3〕 박대우, 윤석현. "VoIP 서비스의 도청 공격과 보안에 관한 연구." 한국컴퓨터정보학회논문지, 제11권 제4호, 2006. 9.

〔4〕 박대우, 서정만. "TCP/IP 공격에 대한 보안 방법 연구." 한국컴퓨터정보학회논문지, 제10권 제5호, 2005. 11.

〔5〕 디지털증거의 무결성, http://caselaw.lp.findlaw.com/cacodes/pen/484-502.9.html. 2007.6.

〔6〕 이규안, 박대우, 신용태. "포렌식 자료의 무결성 확보를 위한 수사현자의 연계관리 방법 연구." 한국컴퓨터정보학회논문지, 제11권 제6호, 2006. 12.

〔7〕 박명순, "휴대폰을 위한 임베디드 시스템", 홍릉과학출판사, 2005.

〔8〕 박상락, "공무원정보보호 인터넷과 컴퓨터수사", 정보통신교육원, 2002.

〔9〕 Williamson,B, "Forensic Analysis of the Contents of Nokia Mobile Phones", School of Computer and Infomation Science Edith Cowan University Perth, Western Australia , 2005.

〔10〕 이규안외, "유비쿼터스환경에서 디지털증거의 무결성 입증방안", 숭실대학교 정보과학대학원, 2006.

〔11〕 이경민, "모바일 포렌식을 위한 CDMA 휴대폰의 데이터 추출 및 분석에 관한 연구", 동국대 대학원, 2007.

〔12〕 장소연, "해시 함수를 이용한 디지털 이미지 워터마킹의 인증 기법 ", 서울산업대 산업대학원, 2004.

〔13〕 QPST. http://www.3gchipsets.co.kr/index.jsp. 2007 5.

〔14〕 정은주, "이동 에이전트 보호를 위한 무결성 검사 메커니즘", 고려대 대학원, 2004.

〔15〕 이강석외 , "AIDE를 이용한 시스템 무결성 구축", 한국정보보호센터, 2004.

저 자 소 개

김 기 환

2003년 (주)테라 네트워크 기술부 부장

2003년 한국 산업기술원, 지방정보화재단 네트워크 강사

2004년 한국방송대 경영학과 (경영학사)

2007년 숭실대학교 정보과학대학원 정보보안학과 (공학석사)

2007년 STG Security 수석컨설턴트

〈관심분야〉 유비쿼터스 보안, 네트워크 보안 시스템, 디지털 포렌식,RFID,SSLVPN,OTP, DRM, 모바일포렌식

박 대 우

1998년 숭실대학교 컴퓨터학과 졸업 (공학석사)

2004년 숭실대학교 컴퓨터학과 졸업 (공학박사)

2000년 매직 캐슬 정보통신 연구소 소장, 부사장

2004년 숭실대학교 정보과학대학원 정보보안학과 겸임조교수

2006년 정보보호진흥원 선임연구원

2007년 호서대학교 벤처전문대학원 정보보호전공 조교수

〈관심분야〉 정보보호, 유비쿼터스 네트워크 및 보안, 네트워크 보안 시스템, CERT, Forensic, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality