휴대폰과 스마트폰의 모바일 포렌식 추출방법 연구

이 정 훈* · 박 대 우**

A Study on Mobile Forensic Extraction Methods of Cellular and Smart Phone

Yi, Jeong Hoon · Park, Dea Woo

〈Abstract〉

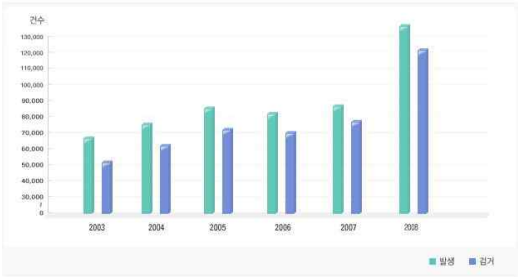
Cellular and Smart phone through the business and real life is associated with an increasing number of information processing, Breaches associated with mobile terminal Tile has occurred and cause Crime and damage. In this paper, Cellular and Smart phone for mobile forensics SYN scheme and JTAG scheme to target Cellular and Smart phone for the extraction of forensic data will be studied. SYN, JTAG approach to forensic analysis indicate with the process, Every Smart phone's OS specific performance and data extraction were compared. In the laboratory, Cell and smart phone with the SYN scheme and JTAG scheme to extract forensic data Improvement compared to the extraction is presented.

Key Words : Mobile Forensic, Cellular Phone, Smart Phone, SYN Scheme, JTAG Scheme

Ⅰ. 서론

고도산업정보화사회에서 업무 처리 정보는 디지털화 되어 사용되며, 저장되고, 3A(Any Time, Any Where, Any Device)를 추구하는 유비쿼터스(Ubiquitous) 시대의 통신은 이동성을 갖춘 무선화, 디지털 장비의 소형화, 멀티미디어화를 통해 자료의 90% 이상이 디지털 형태로 만들어져 디지털 정보의 생산과 유통, 저장되면서 고도 산업화 되어 지고 있다.

경찰청의 사이버 테러대응센터의 자료에 의하면 그림 1과 같이 디지털 정보의 침해사고를 유발하는 사이버 범죄는 매년 증가하고 있으며 이는 경찰청에 신고와 검거 등의 자료임을 감안할 때, 실제 사이버 범죄의 발생 건수는 더 많을 것으로 예상된다.



<그림 1> 사이버범죄 발생 · 검거 현황

방송통신위원회 통계에 따르면 휴대전화를 쓰는 세계 인구는 2008년 말을 기준으로 40억 명, 보급률은 약 61%이다. 2013년에는 세계 보급률이 90% 가까이 치솟을 전망이다. 그 중 최첨단 이동통신 강국인 대한민국은 2008년 기준으로 4,500만 명(보급률 95.2%)이 휴대전화를 쓰

* 호서대학교 벤처전문대학원 IT응용기술학과 석사과정(제1저자)
** 호서대학교 벤처전문대학원 IT응용기술학과 교수(교신저자)

고 있으며, 경제활동인구를 고려하면 보급률은 100%를 웃도는 수준이다. 이와 같이 이동성을 가진 무선 모바일 휴대폰과 스마트폰을 통해서 디지털 정보의 전달과 사용이 빈번하게 이루어지면서, 이동 중에 업무나 실생활과 관련된 정보를 이용하는 도구로서 휴대폰과 스마트폰이 범죄에 이용되고 있다. 모바일 휴대폰과 스마트폰을 통한 범죄는 디지털 무선 정보에 대한 공격을 하여, 침해사고를 유발하고, 피해를 발생시킨다[1].

즉, 유비쿼터스 시대의 고도산업정보화사회의 역기능으로 발생하는 디지털 정보의 침해와 피해에 대한 디지털 관련 범죄를 수사하고, 법정에서 증거자료를 제출하는 디지털 포렌식(Digital Forensic)이 필요하며, 특히 이동성을 갖춘 모바일 휴대폰과 스마트폰에서의 범죄에 관한 증거자료를 분석하고 수집하는 모바일 포렌식(Mobile Forensic)에 관한 연구가 필요하다. 휴대폰의 이동성과 편리성은 범죄자들의 통신수단으로 범죄에 이용되어지고 있으며, 이 결과 휴대폰에 저장된 디지털 자료는 범죄수사 과정에서 휴대폰으로부터 증거를 추출하는 것이 매우 중요한 방법으로 등장하게 되었다[2].

본 논문은 모바일 포렌식에서 휴대폰과 스마트폰을 대상으로 하는 SYN 방식과 JTAG 방식의 휴대폰 분석을 연구한다. 휴대폰과 스마트폰의 증거자료 획득을 위한 디지털 데이터를 추출하는 연구를 할 것이며, 최근에 사용이 급격히 증가하는 스마트폰에 대해서, 범죄와 관련이 되는 증거 추출의 방법에 관한 모바일 포렌식 자료생성에 관한 연구를 한다.

Ⅱ. 관련연구

2.1 디지털 포렌식

디지털 포렌식은 디지털 저장매체에 저장되어 있는 증거자료를 획득하고 분석하여 법정에 제출하기까지의 절차와 방법을 말한다. 포렌식의 사전적 의미는 “법정의”, “변론의” 의미가 되며, 예로서 “forensic medicine”은 “법의학”이라는 뜻이 된다. 한편 디지털 기기의 종류 및 서비스가 매우 다양함으로 표 1과 같이 대상에 따라 분류하여 업무 또는 연구를 진행한다[3].

<표 1> 포렌식 서비스 종류의 상세 분류[3]

명칭	포렌식 서비스 내용
디스크 포렌식	디스크 (파일시스템) 분석
네트워크 포렌식	네트워크 송수신 메일 복구 및 분석, 발송자, 시간, IP 역추적
웹 포렌식	웹 로그, 디지털 콘텐츠 등 분석
모바일 포렌식	휴대폰, 스마트폰, PDA, PMP, MP3, 노트북 기기 등 분석
소스코드 포렌식	소스코드의 저작권, 실행코드와 관계 분석
멀티미디어 포렌식	DRM, Steganography 등 분석
데이터베이스 포렌식	대규모 자료, 부분자료 획득 과정 등 분석

2.2 휴대폰을 이용한 범죄

2.2.1 휴대폰과 스마트폰 범죄 개념

휴대폰과 스마트폰의 높은 보급률과 함께 현금결제, 금융거래가 가능해 지면서 신종범죄의 주역으로 자리 잡고 있다. 휴대폰을 이용한 범죄를 그 양태와 신종범죄에 대한 선행 연구들의 개념규정을 참고하여 정의하여 보면, 이동통신 단말기 및 이동통신 서비스와 관련하여 자기 또는 제3자의 위법적인 이득을 위하여 이동통신 단말기 소유자 및 서비스 활용 자에게 행하는 제반 범법행위라 할 수 있다. 또한 휴대폰을 수단으로 하거나 또는 그 제도를 이용하여 발생된 것으로서 형사적 제재의 대상이 될 수 있는 반사회적 위법행위라고 정의할 수 있다[4].

2.2.2 휴대폰과 스마트폰 범죄의 특성

접근의 용이성은 휴대폰을 이용한 범죄는 전문적인 범죄자가 아닌 일반인도 눈앞의 경제적인 이득을 위해

손쉽게 활용할 수 있다. 비인간성은 사리분별이 부족한 노숙자, 장애인, 노인과 당장 급전이 필요한 사람들에게 접근하여 금전 등의 제공을 미끼로 범죄를 저지른다. 전문성·기술성은 휴대폰 복제 같은 경우 휴대폰에 대한 전문적인 지식과 기술을 갖추고 있어야 가능하다. 광역성·국제성은 명의도용 되거나 불법복제 된 휴대폰의 경우 전국적인 유통망을 통해 거래되거나 우리나라와 동일한 방식의 이동통신망을 쓰는 국가들로 해외까지 반출된다. 비대면성과 익명성은 스팸문자의 경우 휴대폰을 매개로 하여 형성되는 불가시적 공간에서 이루어지고 자신의 신분을 노출시키지 않은 채 활동하는 것이 가능하다. 시간적·공간적 무제한성은 휴대폰 통신망은 공간의 제약을 거의 받지 않고, 24시간 동안 개방되어 있다. 빠른 전파성은 스팸문자는 단한번의 조작으로 수많은 사람에게 동시다발적으로 전파가 가능하다[4, 5, 6].

2.3 모바일 포렌식

휴대폰과 스마트폰, PDA 등의 보급이 늘어나고 유비쿼터스 컴퓨팅이 활성화 되면서 다양한 종류의 멀티미디어 기기가 개발되어 보급되어 이동성과 은닉성이 뛰어나기 때문에 압수수색 시 데이터가 저장되어 있는 소형저장장치가 은닉되어 있는지 여부를 세심하게 조사하는 것도 관건이다[7].

모바일의 분야는 휴대폰을 비롯하여, PDA, 텔레매틱스, 자동차용 블랙박스, 기차용 블랙박스, 선박용 블랙박스, 항공기 블랙박스 등 그 범위가 확장되고 있으나 파일포맷 등의 표준화도 이루어져 있지 않아 데이터 추출 및 분석에는 많은 노력과 연구가 필요하다[8]. 따라서 모바일 포렌식은 휴대폰, 스마트폰, PDA, Laptop, 전자수첩, 디지털 카메라, MP3 플레이어, 휴대용 메모리카드, USB 저장장치 등 모바일기기와 이동장치를 대상으로 하여 범죄나 수사에서 디지털 증거를 수집, 식별, 추출, 보존, 문서화하여 법정에 제출하는 일련의 행위를 말한다[9]. 따라서 범죄 수사 요원들은 범죄 증거의 가능성이 높은 휴대폰과 스마트폰의 증거 확보를 위한 압수 수색을 하여야 한다. 압수 수색한 휴대폰과 스마트폰의 전자파 차단은 무결성을 입증하는 조건이다.

휴대폰과 스마트폰의 압수수색을 진행하기 전에 전원이 켜져 있는 상태라면 휴대폰과 스마트폰의 사용자나 입회인에게 현재 상태를 확인한 후, 전원을 끄고 전자파가 차단되도록 되어 있는 보존봉투에 밀봉 보관하여 그 내용을 기재한 후 서명을 받도록 한다[10]. 이때 휴대폰의 제작사에서 제공하는 통신 프로토콜을 이용하여 컴퓨터와 휴대폰의 데이터를 전송할 수 있으므로 컴퓨터와 통신여부를 확인한 후 통신케이블, 통신 프로그램, 외장형 메모리 등도 압수하여 전자파 차단 봉투에 밀봉하고 그 내용 등을 상세히 기재하여야 한다. 만약 전원이 꺼져 있다면 외관 상태와 휴대폰의 동작 상태 등을 휴대폰의 사용자에게 확인 후에 전자파 차단 봉투에 밀봉 보관하고 그 내용을 기재한다[10].

CDMA(Code Division Multiple Access)폰을 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[11].

2.4 모바일 휴대폰 포렌식 판례

■ 사기범행 공범관계 사건

사기 범행의 공범관계임에도 불구하고, 피고소인을 상대로 자신도 피해자라고 주장하며 고소를 하였다. 수사기관은 피고소인과 고소인 사이에 오고간 핸드폰 문자메시지를 입수하기 위해 피고소인의 핸드폰을 압수하였으나 이미 문자 메시지는 삭제되어 있었다. 수사기관은 압수한 핸드폰의 삭제된 문자 메시지를 복구하고, 이를

근거로 고소인에 대해 무고와 사기를 인지하여 공범인 피고소인과 병합 기소하였다[12].

■ 사생활 침해 사건

2009년 1월 톱스타 J씨는 자신의 휴대폰이 복제된 것 같다며 경찰에 수사를 의뢰했고, 수사결과 J씨 소속사 임원이 사생활을 감시하기 위해 휴대폰을 복제, 문자메시지를 훔쳐본 것으로 판명되었다. 법원은 휴대폰을 복제한 소속사 임원과 직원 2명에게 집행유예 2년에 사회봉사 80시간을 명령했다[13].

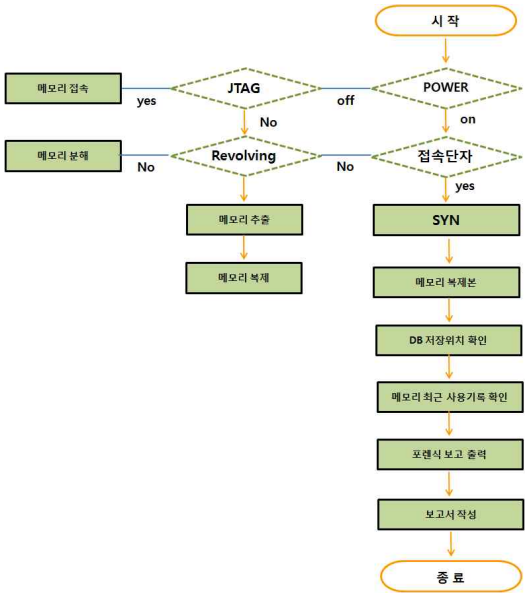
■ 실종・살인 사건

경찰은 연쇄 살인범 K씨가 2006년 12월부터 2008년 12월까지 2년 사이에 경기서남부지역에서 실종된 부녀자 7명을 모두 살해하고 암매장한 것의 관련 증거 자료로 K씨의 휴대전화 사용내역 추적에서 회사원 P모씨가 실종된 장소에서 휴대전화를 사용한 사실을 확인해 자백을 유도하는 정황 증거에 추가할 수 있었던 사건이다[14].

Ⅲ. 휴대폰과 스마트폰 모바일 포렌식 자료 추출

현재 국내에서 모바일 포렌식 중 주로 분석이 진행되고 있는 부분은 휴대폰 분야이다. SMS, 전화번호부, 통화목록, 메모, 스케줄, 사진, 동영상 등의 데이터는 휴대폰 단말기 플래시 메모리에 저장 되어 컴퓨터 등 디지털 기기로 전송하는 방식은 유・무선 방식으로 구분 할 수 있다. 그림 2는 휴대폰과 스마트폰의 자료 추출을 위한 SYN, JTAG방식의 포렌식 분석 과정의 프로세스를 나타낸 것이다.

실험은 휴대폰과 최근에 급속히 사용이 증가하는 스마트폰의 유선방식인 동기신호를 송・수신 후 데이터 전



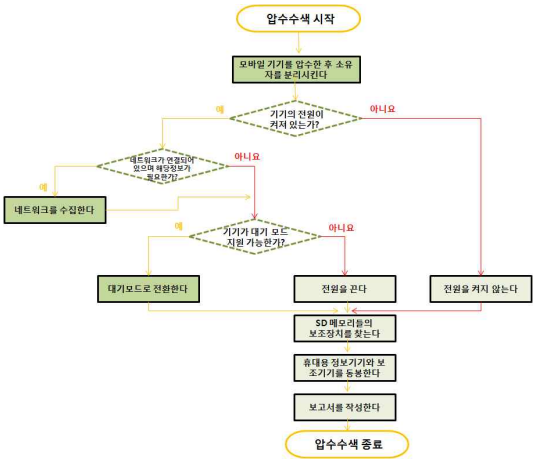
<그림 2> SYN, JTAG 방식의 포렌식 분석 프로세스

송을 하는 SYN 방식과 프로그램의 조정을 위하여 사용하는 JTAG 방식으로 나누어 포렌식 자료를 추출하기 위하여 휴대폰과 스마트폰 제조사에서 제공한 툴과 JTAG 디버거를 이용하여 실험을 실시한다.

3.1 압수수색

휴대폰과 스마트폰에서 증거 자료를 추출하기 위해서는 압수수색을 실시하여야 한다. 그림 3은 휴대폰과 스마트폰 압수수색 절차를 나타낸 것이다.

휴대폰과 스마트폰을 압수 수색 후에 포렌식 증거 분석을 실시 할 때, 삭제된 자료를 복구 할 필요가 있는지 결정 후, 삭제된 자료를 복구할 필요가 있을 경우, 스마트폰의 자료를 다운받아 복제하거나 원본성을 입증 할 수 있는 해시 함수 값을 적용한 후에 복사본을 생성한다. 삭제된 자료를 복구하기 위해 복제 및 복사본을 생성하였을 경우 복제 및 복사본에 대해 검사 및 복구를 시행한다. 전파차폐장치를 사용하여 통신을 차단하고 쓰기방



<그림 3> 휴대폰·스마트폰 압수수색 절차[15]

지장치를 사용하여 노트북 및 분석 컴퓨터에 연결한다. 노트북 및 분석 컴퓨터에서 스마트폰과 상호작용하는 응용프로그램을 실행시켜 스마트폰에 저장된 정보를 이동한다. 추출된 스마트폰 자료의 복사본 또는 저장한 증거파일의 해시 값을 확인 후 보관한다.

3.2 포렌식 실험 환경

휴대폰과 스마트폰의 포렌식 자료 추출을 위하여 그림 4와 같이 실험 환경을 구성하였다. 표 2는 스마트폰의 OS별 성능을 비교 분석 한 것이다.

<그림 4> 휴대폰·스마트폰 포렌식 자료 추출 실험 환경

(1) 실험 PC
- CPU : Intel(R) Core(TM) i3 CPU 530 @ 2.93GHz
- OS : Windows 7 Ultimate K
- RAM : 4.00GB
- HDD : 450 GB

(2) 스마트폰(윈도우모바일기반)
- 명 칭 : SCH-M490(Anycall)
- 통신사 : SKT
- CPU : PXA270 570Mhz
- Memory : ROM- 256MB, RAM-64MB
- OS : Windows Mobile 6.0
- 통신방식: WCDMA / GSM
- 사양 : 3.3형 LCD 65K / TFT LCD (Touch 지원)
- 카메라 : 500만화소 카메라 / Auto Focus 지원 영상전화/플래시
- 슬롯 : MicroSD 카드 슬롯 (MicroSD/MicroSDHC 지원)
- 기능 : 전자다이어리기능, 위성DMB 기능 지원, Push Mail 기능 등
- 제조사 : 삼성전자(주)

(3) 스마트폰(안드로이드기반)
- 명 칭 : SHW-M110S(Anycall)
- 통신사 : SKT
- CPU : 1GHz
- Memory : RAM-512MB
- OS : 안드로이드
- 통신방식: WCDMA / GSM
- 사양 : 4.0형 Super AMOLED / Full Touch Bar
- 카메라 : 500만화소 카메라 / Auto Focus 지원 CMOS/
- 슬롯 : MicroSD 카드 슬롯
- 기능 : 구글모바일서비스, Internet Browser 지원, 홈스크린 위젯 기능 등
- 제조사 : 삼성전자(주)

(4) 휴대폰
- 명 칭 : SEC-SPHW2700 (Anycall)
- 통신사 : KTF
- 제조사 : 삼성전자(주)

(5) 추출도구
- SYN 방식 : PC Manager Plus, MITs wizard, Kies
- JTAG 방식 : Trace32, JTAG 디버거

(6) 케이블
- SYN 방식 : USB 케이블
- JTAG 방식 : 자체제작 케이블

(7) 스마트폰의 OS별 성능 비교

<표 1> 공격도구의 유형 및 특성

	아이폰	안드로이드	심비안	윈도우 모바일
네이티브 개발을 위한 언어	Objective-C	Java	C++	C++, C#, VB. Net
디지털 서명 서포트	있음	없음	있음	있음
플랫폼의 성숙도	미숙	미숙	성숙	성숙
App 설치 방법	앱 스토어, iTunes	미공개	PC Suite	ActiveSync
공식 에뮬레이터 제공	있음	있음	있음	있음
원격 디버깅	가능	가능	좋음	가능
터치스크린 지원	멀티 터치	싱글 터치	싱글 터치	싱글 터치
응용 가용성과 다양성	낮음	낮음	높음	높음
기반 아키텍처	Mac OS X	Linux	Symbian	Windows
Flash 가용성	없음	없음	있음	있음
Java 가용성	없음	있음	있음	있음

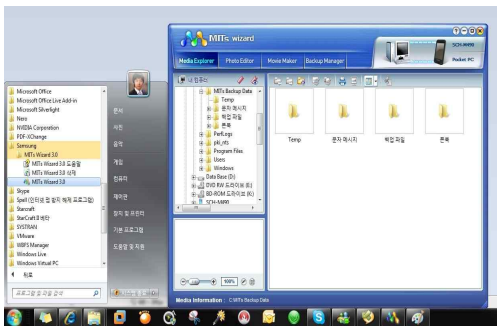
3.3 SYN 방식 포렌식 자료 추출 설정

SYN 방식으로 포렌식 자료를 추출하기 위해 휴대폰과 스마트폰에 대한 입출력 단자에 링크(USB)케이블을 연결하여야 한다. 휴대폰과 스마트폰의 입출력 단자의 기능은 충전기를 위한 기능, 핸즈프리를 위한 기능, 자료 전송을 위한 기능을 지원하기 위하여 휴대폰 제작사들은 공통으로 사용하는 인터페이스를 제작하여 공급하고 있으며, 자료 전송을 위한 기능을 이용하여 사용자들에게 휴대폰 사진이나 메시지, 전화번호를 컴퓨터에 저장하거나 전송할 수 있도록 지원하여 개인 블러그, 홈페이지에 이용할 수 있도록 하고 있다.

SYN 방식은 통신의 프로토콜 중에서 SYN 신호를 통하여 동기신호의 교환이 이루어 진후에 자료를 송·수신하는 방식으로 휴대폰과 스마트폰의 제작사에서 제공하는 프로그램을 이용한다.

그림 5는 휴대폰을 제작사에서 지원하는 SYN 통신 프로그램 PC Manager Plus를 실행 시켜 휴대폰에 연결시킨 모습이다. 그림 6은 스마트폰(윈도우모바일)을 제작사에서 지원하는 SYN 통신 프로그램 MITs wizard를 실행 시켜 휴대폰에 연결시킨 모습이다.

<그림 5> 휴대폰 SYN 통신 프로그램



<그림 6> 스마트폰(윈도우모바일) SYN 통신 프로그램

휴대폰과 스마트폰을 이용하여 촬영을 하거나 수신된 자료를 컴퓨터에 저장하기 위해서 휴대전화 단말기의 입출력 단자 접속 표준을 사용하도록 권고하고 있다.

사용자의 조작 또는 프로그램의 버그가 발생하였을 경우 휴대폰 진단모드에서 프로그램의 수정을 위하여 제공되는 기능으로 자료 전송을 위하여 24핀 접속방식을 사용하면서 데이터 통신을 위하여 3번 DSR, 13번 RXD, 14번 TXD, 17번 DCD, 18번 RI, 20번 RFR:RTS, 23번 CTS, 24번 DTR 8핀, 기타 4핀 모두 12핀의 번호를 사용하고 있다[10].

SYN 방식을 위하여 제작사에서 제공하는 데이터 통신은 13, 14번을 이용하고 있다. S사에서는 PC Manager Plus(휴대폰), MiTs wizard(윈도우모바일), Kies(안드로이드) 프로그램을 제공하고, 제작사의 프로그램을 통하여 자료를 송·수신할 수 있다. SYN 통신방식에서는 SMS, MMS, 사진, 동영상 등의 자료만 송·수신이 가능할 뿐 삭제되거나 은닉된 자료는 볼 수 없다.

3.4 SYN 방식 휴대폰 자료 추출 분석

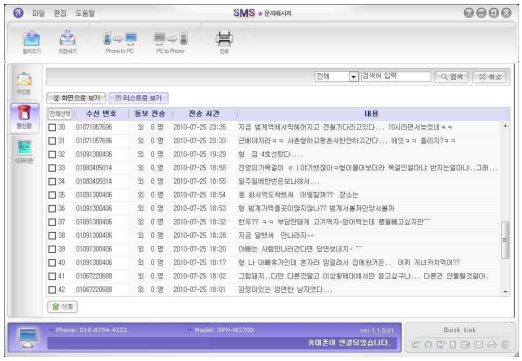
제조사에서 제공하는 툴을 이용하여 그림 7, 8, 9와 같이 휴대폰과 스마트폰의 SMS, 사진 자료를 추출한다.

휴대폰과 스마트폰의 전원을 켜진 상태에서 메시지를 확인 할 수 있고, 저장 된 사진을 추출 할 수 있다. 하지만 삭제 된 자료는 추출 해 낼 수 없다.

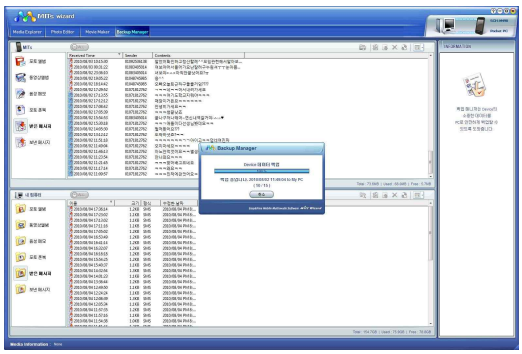
3.5 JTAG 방식 포렌식 자료 추출

휴대폰과 스마트폰 전원불량으로 작동이 안 되거나, 자료가 삭제되어 복원을 통한 정밀 분석을 필요로 하는 방식을 JTAG 방식이라 한다.

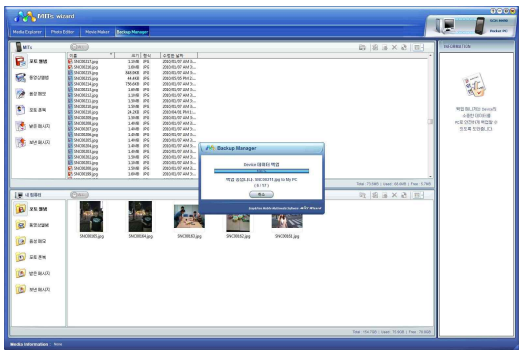
휴대폰에는 24개의 포트가 존재하는데 공통으로 사용하는 포트 번호는 USB 통신을 위한 전원과 자료의 핀 번호는 10, 12, 13, 14, 15, 16, 19, 21, 22번만 사용하고 있으며 나머지는 회사별로 JTAG 핀 맵과 다른 정보를 위한



<그림 7> 휴대폰 제조사의 툴을 이용한 SMS 추출



<그림 8> 스마트폰(윈도우모바일) 제조사의 툴을 이용한 SMS 추출



<그림 9> 스마트폰(윈도우모바일) 제조사의 툴을 이용한 사진 추출

번호를 숨기고 있다[10]. 스마트폰 JTAG 방식은 자료 추출은 가능하지만 파일 포맷을 분석이 어려우며, 휴대폰 JTAG 방식을 기반으로 연구 되고 있다.

일반적으로 JTAG 디버거는 CPU의 동작을 직접 내부

에서 제어하여 로컬버스에 문제가 있는 타켓 시스템에서도 메모리나 입출력장치를 읽고 쓸 수 있는 기능을 이용하여 그 원인을 찾아낼 수 있는 장비다. JTAG 기능으로는 디바이스 내에서 모든 외부와의 연결점을 가로채고, 각각의 셀은 시리어 쉬프트 레지스터를 형성하기 위해 서로 연결된다. JTAG는 디바이스의 핀 상태를 읽어내고, 내부 신호의 상태를 읽어내기 위한 기술로서 보드 테스트, 디버깅에 활용된다. 또한 논리회로와 플래시 메모리의 퓨징과 마이크로프로세서의 코어에 직접 접근할 수 있는 방법을 제시함으로 소스 레벨 디버깅에도 사용할 수 있다. JTAG 인터페이스는 핀에 의해서 제어되며 회로의 배선과 소자의 전기적 연결 상태의 테스트, 디바이스간의 연결 상태 테스트, 플래시 메모리의 조작 등 이라고 할 수 있다. 휴대폰 자료를 추출하기 위해서는 휴대폰의 JTAG 핀을 찾고, JTAG 디버깅 환경을 설정하고, 메모리 바이너리 자료를 획득한다.

JTAG 방식을 이용하여 SRAM과 플래시 메모리 부분까지 자료를 추출하는 방법은 각 제작사 및 제품별로 휴대폰의 PCB(Printed Circuit Board)에 JTAG의 통신을 위한 포트가 존재하게 되는데 이러한 포트를 찾아내어 JTAG 핀 맵과 연결하므로 통신을 위한 인터페이스가 완성된다. 모든 영역의 자료를 덤프 하는 기법으로 안테나 차단이 되는 등 디지털 증거의 무결성을 보장하고 은닉되거나 삭제된 자료를 추출한다[10]. 추출된 자료는 2진수로 되어 있으므로 회사별로 공통된 수를 검색하고 메시지인 경우 헤더의 부분과 끝 부분의 숫자를 파악한 다음 동일한 숫자의 반복횟수별로 자료를 절단하고 조합하여 필요한 정보를 추출한다. 표 3는 스마트폰(안드로이드)의 각 애플리케이션 데이터베이스 경로를 나타낸 것이다. 데이터베이스에는 해당 파일의 경로만 저장된다.

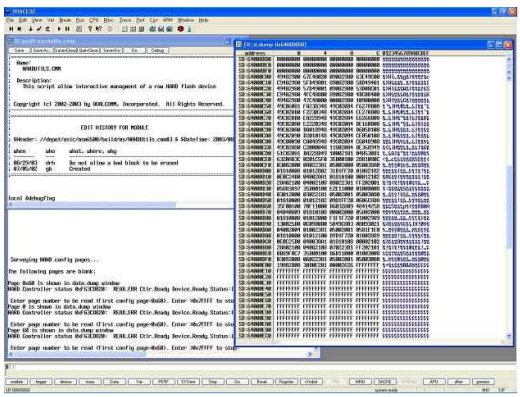
3.6 JTAG 방식 휴대폰 자료 추출 분석

그림 10은 Trace32의 프로그램을 이용하여 추출 된 자료이다. 추출 된 자료를 보면 16진수로 되어 있으므로 이

<표 3> 안드로이드 데이터베이스 경로

애플리케이션	SQLite Database
SMS	\data\data\com.android.providers.telephony\databases \mmssms.db
MMS	\data\data\com.android.providers.telephony\databases \mmssms.db
웹브라우저 검색어	\data\data\com.android.browser\databases\browser.db
웹브라우저 북마크, 히스토리	\data\data\com.android.browser\databases\browser.db
전화번호부	\data\data\com.android.providers.contacts\databases \contacts2.db
통화내역	\data\data\com.android.providers.contacts\databases \contacts2.db
멀티미디어	\data\data\com.android.providers.media\databases\external_숫자.db

를 파일에 맞도록 구분하고 정리를 하여야 한다. 분석결과를 보면 전화번호부의 경우 전화번호부 1개에는 40byte의 메모리를 할당하였다. 시작은 01로 끝은 00으로 하였다. 전화번호부의 단축키를 이용하기 위하여 16진수 4개를 할당하였으며, 단축키가 없는 경우에는 FFFF로 표시를 하였다. 휴대폰의 사용자에 대한 구분을 위하여 필드인덱스는 00은 집전화, 01은 휴대폰, 02는 직장전화, 03은 기타로 구분하고, 06은 메모를 할 수 있도록 하였다[10].



<그림 10> Trace32를 이용하여 추출 된 자료

휴대폰에서 복원된 사진의 일부 화면이 보이지 않게 되는 것은 저장된 자료의 일부가 덮여 씌어 지거나 다른 자료에 의하여 복원이 불가능하게 되었지만 수사에 필요한 단서는 충분하게 추출할 수 있다. 동일한 방법으로 메시지에 대한 복원도 수행 할 수 있다. 메시지는 메모리의 할당영역에 속해 있는 내용에 대하여 추출할 수 있다.

5B 00을 플래그로 사용하며 실제 자료는 삭제되지 않았음에도 휴대폰은 디스플레이 되지 않도록 하는 것은 메시지인 경우 1.6Kbyte의 저장 공간을 제공하면서 삭제된 문자임을 표시하기 위해서다. 6F에서는 파일의 구분을 위하여 파일 번호를 사용하는 플래그이며, 7B 00은 메시지 전체의 길이임을 알 수 있다. 윈도우모바일기반 스마트폰과 안드로이드기반 스마트폰은 JTAG 핀을 찾고, JTAG 디버깅 환경을 설정하였으나, 스마트폰 포렌식 자료의 추출은 성공하고, 자료의 분석에는 실패하였다.

Ⅳ. 휴대폰과 스마트폰의 SYN 방식과 JTAG 방식의 포렌식 비교

4.1 휴대폰과 스마트폰의 SYN 방식과 JTAG 방식 포렌식 비교

SYN 방식을 이용하여 자료를 추출하는 휴대폰과 스마트폰 분석 방식은 삭제되지 않은 자료를 추출하기에 유용하지만 삭제된 자료를 추출하는 것은 불가능하다. 일부 휴대폰과 스마트폰에서 수사에 필요한 자료가 추출되었지만, 삭제된 것이 아니라 자료의 주소가 변경되어 참조주소를 추적하여 추출되는 것이다.

SYN 방식과는 달리 전원이 꺼져 있는 상태에서 분석이 가능한 JTAG방식은 삭제된 자료를 복원하여 추출 하는 것이 가능하다. 본 연구결과 휴대폰에서 문자 메시지는 삭제된 메시지의 모든 것이 복원되었으나, 일부 휴대폰에서 메시지의 전송이 빈번한 경우에 복원되는 문자의 량이 현저히 낮아지는 것을 확인하였다.

휴대폰의 JTAG 방식을 통하여 추출된 데이터는 SYN 방식에서는 추출하지 못한 삭제된 데이터에 대한 추출과 복원 능력이 뛰어나지만, 스마트폰은 파일 포맷 분석기술과 자료의 분석이 어려워 추출하지 못하였다. 표 4는 휴대폰과 스마트폰의 SYN 방식과 JTAG 방식 포렌식 추출을 비교한 것이다.

<표 4> 휴대폰과 스마트폰 포렌식 자료 추출 비교

	SYN 방식	JTAG 방식
휴대폰	- 활성화 된 SMS, MMS, 전화번호부, 통화내역, 멀티미디어 자료 포렌식 추출 가능.	- SMS, MMS 전원 재부팅 시에는 순차적으로 자동 삭제 됨. - 삭제된 SMS, MMS, 전화번호부, 통화내역, 멀티미디어 복원 추출 및 분석 가능
스마트폰 (윈도우모바일)	- 활성화 된 SMS, MMS, 전화번호부, 통화내역, 멀티미디어 자료 포렌식 추출 가능. - 웹브라우저 검색어, 웹브라우저 북마크, 히스토리 자료 포렌식 추출 가능.	- 메모리에 저장된 자료에 대한 단자 찾기가 어려움 - 탈옥, 해킹 시 구조변경에 따른 분석이 어려움 - 삭제된 SMS, MMS, 전화번호부, 통화내역, 멀티미디어, 웹브라우저 검색어, 웹브라우저 북마크, 히스토리 복원 추출이 가능하지만 분석 어려움.
스마트폰 (안드로이드)	- 활성화 된 SMS, MMS, 전화번호부, 통화내역, 멀티미디어 자료 포렌식 추출 가능. - 웹브라우저 검색어, 웹브라우저 북마크, 히스토리 자료 포렌식 추출 가능.	- 메모리에 저장된 자료에 대한 단자 찾기가 어려움 - 탈옥, 해킹 시 구조변경에 따른 분석이 어려움 - 삭제된 SMS, MMS, 전화번호부, 통화내역, 멀티미디어, 웹브라우저 검색어, 웹브라우저 북마크, 히스토리 복원 추출이 가능하지만 분석 어려움.

만약 휴대폰이나 스마트폰의 작동이 불능이고 단말기기가 파손되었을 때는, 메모리를 덤프하고, 덤프 된 데이터에서 휴대폰에 쓰이는 많은 프로토콜 및 자료의 패턴을 분석하고 연구하여 포렌식 데이터를 추출하는 방법이 있다. 현재 대부분의 휴대폰은 제품의 크기 및 제조공정의 편리성 때문에 BGA 타입을 이용하고 있다. 휴대폰의 NAND 플래쉬 메모리를 PCB보드에서 분리하는 작업은

자동화 기계를 이용하여 사용한다. BGA 리볼링 작업이 완료된 NAND 플래쉬 메모리는 데이터를 추출하는 장비인 FlashPAK 장비를 이용하여 데이터를 추출하게 된다. 보통 FlashPAK 장비에는 메모리를 다운 받을 수 있는 프로그램이 장착되어 있고, 만약 플래쉬 메모리의 추출 프로그램이 없는 경우에는 회사의 프로그램을 다운로드 받아 설치하면 된다. 추출된 데이터는 이진수이므로 이를 16진수 혹은 가시적인 데이터로 디버깅 작업 변환을 하여야 한다.

4.2 포렌식 추출 개선 방안

휴대폰과 스마트폰의 SYN 방식의 경우 활성화된 데이터를 추출 할 수 있다. 하지만 통화내역 등 삭제 된 자료까지 복구를 하여야 범죄와 관련 된 증거 자료로 수집되어져야 된다.

SYN 방식을 사용하여 휴대폰과 스마트폰에서 삭제된 전화번호, 주소록, 일정표, 사진, 동영상에 제한되어 있는 것을 SYN 신호에 플래시 메모리의 통화내역, SMS, MMS, 전화번호부, 멀티미디어 등에 대한 자료와 삭제된 자료를 추출 할 수 있도록 한다. JTAG 방식을 통하여 휴대폰과 스마트폰에서 데이터를 추출하는 방법은 JTAG 핀 맵에 대한 구성에 대한 분석이 단말기 별로 필요하다. 하지만 JTAG 핀 맵 구성은 휴대폰의 제작사 별로 서로 상이하고 회사 기밀로 규정이 되어 있으므로 파악하기 어렵다.

휴대폰과 스마트폰의 JTAG 방식을 개선하기 위하여 JTAG 핀 맵을 수기로 검색하여 추출하는 것이다. 스마트폰 JTAG 방식을 개선하기 위하여 파일 포맷기술을 익히는 교육이 필요하다. 파일포맷기술을 이용하여 자료분석을 추출할 수 있을 것이다. 새로운 휴대폰이 출시된다고 하더라도 통신 포트는 항상 개방되어 있기 때문에 지속적인 연구를 진행 한다면 휴대폰과 스마트폰에 저장된 데이터와 삭제된 데이터를 추출하는 모바일 포렌식에 많은 도움이 될 것이다.

Ⅴ. 결론

본 논문은 휴대폰과 스마트폰을 압수수색 된 것으로 가정하고, 휴대폰과 윈도우모바일기반 스마트폰, 안드로이드기반 스마트폰에 대한 SYN 방식과 JTAG 방식의 포렌식 기술을 이용하여 데이터를 추출하여 비교 분석하였다.

휴대폰과 스마트폰에서 SYN 방식 포렌식 자료 추출은 삭제되지 않은 데이터를 추출하기에 유용한 방법이지만 삭제된 데이터를 추출이 어려웠다. 휴대폰의 JTAG 방식은 삭제된 데이터가 대부분 추출되었으며, 추출된 데이터는 분석과정을 거쳐 시각화되어 수사에 활용되고 있음을 입증할 수 있었다. 스마트폰 JTAG 방식은 삭제되지 않은 자료는 추출하였으나, 추출된 자료를 분석과정을 거쳐 시각화되는 것에는 실패 하였다.

향후 연구로는 스마트폰의 새로운 모델에 맞는 디지털 데이터 추출 기술 연구와 휴대폰과 스마트폰의 제작사별로 서로 다른 핀 맵 구조를 사용하고 있는데 따른 파일 포맷의 표준화 추출과 분석에 관한 기법을 연구하여, 모바일 포렌식 연구 발전에 기여 할 것이다.

참고문헌

[1] 이영숙・김지연, “스마트폰 보안 기술 분석," 디지털산업정보학회, 디지털산업정보학회논문지, 제6권, 제2호, 2010.

[2] 이규안・박대우・신용태, “포렌식자료의 무결성 확보를 위한 수사현장의 연계관리 방법 연구," 한국컴퓨터정보학회, 한국컴퓨터정보학회논문지, 제11권, 제6호, 2006, pp. 175-184.

[3] 이규안, “JTAG 방식을 이용한 모바일 포렌식 기법 연구,” 숭실대학교대학원 박사학위논문지, 2009.

[4] 신성원, “휴대폰 범죄의 실태 및 효율적 대응방안에 관한 연구," 한국콘텐츠학회, 한국콘텐츠학회논문

지, 제6권, 제9호, 2006, pp. 75-84.
[5] 백광훈, “사이버범죄에 대한 ISP의 형사책임에 관한 연구," 한국형사정책연구원, 2003.
[6] 강동범, “사이버범죄와 형사법적 대책," 한국형사정책연구원, 한국형사정책연구원 제25회 형사정책세미나 자료집(사이버범죄의 실태와 대책), 제42호, 2000.
[7] 권준희・김성림, “유비쿼터스 환경에서 상황 데이터 기반 모바일 콘텐츠 서비스를 위한 추천 기법," 디지털산업정보학회, 디지털산업정보학회논문지, 제6권, 제2호, 2010.
[8] 이성진, “디지털 포렌식스 기술 발전 방안," 한국디지털포렌식학회, 한국디지털포렌식학회논문지, 제1권, 제1호, 2007, pp. 1-22.
[9] 김기환・박대우, “모바일 포렌식 자료의 추출과 무결성 입증 연구," 한국컴퓨터정보학회, 한국컴퓨터정보학회논문지, 제12권, 제6호, 2007, pp. 177-185.
[10] 이정훈・박대우・이규안, “SYN 방식과 JTAG 방식의 모바일(휴대폰) 포렌식 연구," 한국컴퓨터정보학회, 한국컴퓨터정보학회 학술대회, 2010.
[11] 경찰청 사이버테러대응센터, “제2회 디지털 포렌식 세미나 발표자료," 한국디지털포렌식학회, 2007.
[12] 대검찰청, 2007년 검찰 올해의 사건 3, 과학수사사례.hwp, 2007.
[13] 스포츠조선, ’전지현 휴대폰 복제 사건,’ 스포츠조선, http://sports.chosun.com/news, 2009. 1. 29.
[14] 연합뉴스, 김동규, ’강호순 범행 뒤 첫 통화는 애인... 패턴 일정,’ 연합뉴스, http://app.yonhapnews.co.kr, 2009. 02. 05.
[15] 경찰청, “유형별 증거분석 표준절차," 디지털증거처리 표준가이드라인, 2006, p. 42.

■ 저자소개 ■

이 정 훈
Yi, Jeong Hoon

2009년 3월~현재 호서대학교 벤처전문대학원 석사과정
2009년 2월 호서대학교 정보통신공학과(공학사)

관심분야 : 포렌식, 정보보호, 금융정보보안, 네트워크보안, IT-Convergence
E-mail : yyyjjhh@paran.com

박 대 우
Park, Dea Woo

2007년 3월~현재 호서대학교 벤처전문대학원 조교수
2006년 2월 정보보호진흥원(KISA) 선임연구원
2004년 6월 숭실대학원 정보과학대학원 정보보안학과 겸임조교수
2004년 2월 숭실대학교 컴퓨터학과 (공학박사)
1998년 2월 숭실대학교 컴퓨터학과 (공학석사)

관심분야 : 정보보호, 유비쿼터스 네트워크 및 보안, 보안 시스템, CERT/CC, e-Discovery, Forensic, VoIP 보안, 이동통신 및 WiBro 보안, IT-Convergence, Cyber Reality
E-mail : prof1@paran.com

논문접수일 : 2010년 8월 7일
수 정 일 : 2010년 8월 16일(1차), 8월 26일(2차)
게재확정일 : 2010년 9월 2일