모바일 포렌식의 디지털 증거 획득을 위한 표준 모듈 개발

*장성균, **조인휘
한양대학교 대학원 전자컴퓨터통신공학과
e-mail : *sunggyun@mdstec.com, iwjoe@hanyang.ac.kr*

Development of Standard Module for Collecting Digital Evidence of Mobile Forensic

*Sung-Gyun Jang, **In-Whee Joe
Department of Electronics and Computer Engineering
Hanyang University

Abstract

Recently, our lives have become more convenient and our work more efficient as a result of these cell phones. On the other hand, they have also caused diverse side-effects, including threats of blackmail with invasion of privacy, disclosure of personal information, as well as security breaches, and an overall increase in distrust between people. Recognizing the need to quickly collect digital evidence with an increase in cell phone crimes, this paper proposes to develop such standard module.

I. 서론

정보통신부는 '정보통신 일등국가' 건설로 다져진 IT 강국의 위상을 기반으로 유비쿼터스 사회를 조정하기 위한 정책을 추진하면서 '다이나믹 u-코리아'를 슬로건으로 멀티미디어 기능을 갖추며 신용카드, 금융계좌, 전자화폐 등을 편리하게 사용할 수 있는 환경을 구축하고, 사회안전망 강화를 위해 위치정보를 활용한 치매.독거노인 응급치료서비스와 가정의 도난.화재 등에 대처하기 위한 재난 대응서비스를 제공하기도 한다. 이러한 휴대폰 사용으로 생활이 편리해지고 효율적인 업무추진이 가능해졌지만 개인정보 침해로 인한 공갈 및 협박, 정보유출, 서비스 거부 공격 등 보안 사고에 대한 많은 취약점으로 인해 정보화 역기능이 점차 심각해지고 그에 따른 불신도 가중되면서 사회의 질서를 파괴하는 범죄로서 인식되고 있어 심각한 사회문제가 될 우려가 있다. 휴대폰 관련 범죄는 전 세계적으로 급증하고 있는 추세이며 이에 따라 모바일 포렌식도 활발한 움직임을 보이고 있다. 하지만 아직까지 우리나라는 모바일 포렌식에 대한 전문적인 지식 및 분석 도구가 없어서 많은 어려움에 부딪히고 있는 실정이어서 디지털 자료 증거의 확보 및 분석 그리고 무결성을 입증하는 것이 쉽지가 않다[1].

본 논문은 휴대폰 제조사마다, 생산되는 휴대폰마다 서로 다른 플래시 메모리를 사용하더라도 각각의 별도의 분석 도구 필요 없이 디지털 증거를 빠르게 확보할 수 있게 개발한 표준 모듈을 소개하고, 휴대폰의 변화에 따라 계속적으로 지원하기 위한 모바일 포렌식 분석 도구의 업그레이드를 빠르게 할 수 있는 방안을 제시하는데 그 목적이 있다.

II. 본론

본 논문은 디지털 증거 획득에서 가장 중요한 User data를 획득하는 방법을 제시하고자 한다. 디지털 증거 획득을 하는 방법에는 Logical, Physical 두 가지로 나눠지게 된다. Logical방법은 휴대폰의 USB 또는 Serial을 통해 PC로 복사하는 방법이며 휴대폰 제조회사 마다 적합하지 않아 증거확보에 어려움이 있고, 상용화된 프로그램은 업데이트가 빨리 되지 않는 큰 단점이 있으며 업데이트 시 많은 비용을 지불해야 한다. Physical

방법은 Hardware 적인 도구를 통해서 플래시 메모리를 직접 읽는 방식이다. 휴대폰의 플래시 메모리를 직접 떼어내서 ROM WRITE 도구로 읽어 내는 방법인데, 떼어낸 플래시 메모리는 휴대폰에 다시 붙여서 사용할 수가 없기 때문에 휴대폰을 폐기처리 해야 한다는 것이다. 본 논문은 새로운 방법인 JTAG 을 이용하여 플래시 메모리를 휴대폰에서 떼어 내지 않고 증거를 획득하는 방법이다. 이 방법을 사용하면 휴대폰에서 플래시 메모리를 떼어내지 않아도 되며 따라서 휴대폰을 폐기하지 않고 빠른 시간 내에 디지털 증거 자료를 획득 할 수가 있다. 휴대폰 제조사와 플래시 메모리의 종류에 따라 User data 확보하는 방법이 다양하며, 또한 다양한 방법으로 인해 증거 획득의 방법에 대한 개발이 복잡 해 질 수 있지만, 이를 표준화 시켜 증거 획득 확보의 어려움을 해소하기 위한 표준 모듈(SMART: Standard Module of extrAction for useR daTa)을 개발하였다.

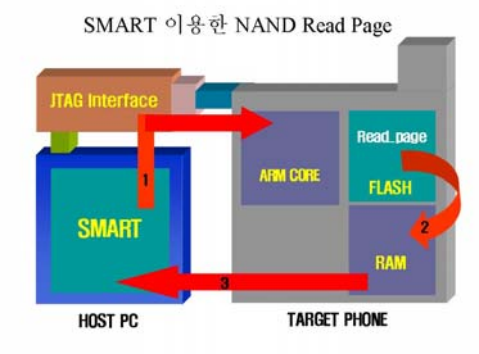

그림 1. 설계

국내에서 휴대폰 개발의 표준 JTAG 도구인 TRACE32의 Script Language를 이용하여 증거물 획득을 하도록 구현하였다.

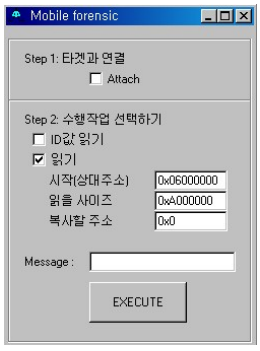

그림 2. SMART

SMART는 NAND Controller의 Register를 직접 제어했기 때문에 CDMA 또는 WCDMA의 Qualcomm 프로세서 사용한 휴대폰이라면 표준 모듈로 사용할 수 있으며, 휴대폰의 플래시 메모리 Size나 Cycle이 다를 경우를 대비해서 Parameter 값으로 조절하도록 설계되어 증거 획득의 어려움을 최소화하도록 했다. 새로운 휴대폰이 계속해서 개발되어 상용화 되고 있는 상황에서 휴대폰 종류별로 별도의 분석 도구 개발 및 업데이트가 힘든 환경이지만 SMART는 Text기반으로 된 Script Language이기 때문에 연구원이 손쉽게 휴대폰 환경에 맞게 변경 할 수 있다.

Ⅲ. 성능 평가

아래는 RANDOM하게 제조 회사별로 휴대폰을 선택해 SMART를 적용해 보았다. 디지털 증거 획득을 확보하는데 있어서 가능했음을 입증하였다.

표 1. 제조사별 증거 확보 여부

제조사	모 델	증거 확보 여부
LGE	SV550	증거 획득 가능
SAMSUNG	V700	증거 획득 가능
PANTECH	U160	증거 획득 가능

Ⅳ. 결론 및 향후 연구 방향

2006년 조사에 의하면 전 세계 인구의 40%가량인 20억 명이 휴대폰을 사용하고 있다고 한다. 우리나라는 3500만 명에 달하는 사람들이 휴대폰을 사용하고 있다. 그에 따라 모바일 포렌식도 점점 더 필요성과 전문성이 요구되고 있는 실정이다. 모바일 포렌식 증거 확보에 필요한 표준 모듈의 개발은 현 시대의 요구에 부합하는 것이 될 것이다. 그에 이번 SMART 실험 및 평가는 휴대폰 제조사 및 모델이 달라도 증거 확보에 있어 접합성이 증명되었음에 의미가 있다. 향후에는 CDMA 또는 WCDMA 휴대폰에 국한이 되어 있는 SMART를 GSM 휴대폰에도 적용시키는 연구와 더불어 디지털 증거를 확보하는 것뿐만 아니라 SMS, 동영상, 사진과 같은 User data를 분석 및 무결성 입증 가능 표준 모듈이 되도록 추가 연구를 진행할 예정이다.

참 고 문 헌

[1] 김기환외, "모바일 포렌식에서의 무결성 입증방안 연구" 한국 컴퓨터정보학회 제 15권 제1호, 2007. 6

[2] 정익래외, "디지털 포렌식 기술 및 동향" 전자통신 동향분석 제 22권 제1호, 2007. 2

[3] Paul McCarthy,Dr Jill Sla,"Forensic Analysis of Mobile Phones" University of South Australia, 2005. 10

[4] Andrew N Sloss 외, "ARM SYSTEM DEVELOPER'S GUIDE", 사이텍미디어, 2005. 2

[5] Paul McCarthy, "Forensic Analysis of Mobile Phones" University of South Australia, 2005. 10