JTAG을 이용한 휴대폰 포렌식 데이터 수집

*김건우, **류재철
*한국전자통신연구원, **충남대학교
*wootopian@etri.re.kr, **jcryu@home.cnu.ac.kr

Forensic Data Acquisition on Cell Phone using JTAG Interface

*Keonwoo Kim, **Jae-Cheol Ryu
*ETRI, **Chungnam National University

Abstract

With the role of cell phones in today's society as a digital personal assistant as well as the primary tool for personal communication, it is possible to imagine the involvement of cell phones in almost any type of crime. The progression of a criminal investigation can hinge on vital clues obtained from a cell phone. This paper will be concentrated on CDMA system phones and focus on the data extraction for cell phone forensics. Especially, the data acquisition method of JTAG interface access to memory chip will be covered.

I. 서론

오늘날 휴대폰의 기능 향상은 범죄 행위에 대한 조사 과정에서 많은 정보를 제공하는 수단이 되고, 이러한 정보들이 증거로서 사용될 수 있다. 휴대폰 내에 저장되는 정보는 연락처, 통화목록, 통화시간, 착발신 메시지, 사진, 동양상, 음성녹음, 일정, 메모, 인터넷 브라우저 정보, 다운로드 파일 등이 있다.
휴대폰에 저장된 데이터를 획득, 분석해서 증거를 찾아내는 휴대폰 포렌식 기술은 접근방식에 따라서 장단점이 있다. 소프트웨어 포렌식 툴을 이용하면 폰내의 데이터를 비교적 쉽게 추출할 수 있다. JTAG 과 같은 low-level 접근방법을 이용하면 데이터 수집을 위한 별도의 장비가 필요하지만 가장 완벽하게 모든 데이터를 추출할수 있다. 본 논문에서는 휴대폰 데이터를 추출하는 방법중 JTAG 인터페이스를 이용한 폰 데이터 획득에 관해서 논한다.

II. 휴대폰 데이터 획득 방법

유효한 증거 데이터를 찾기 위해서는 우선 휴대폰에 저장된 데이터를 획득하는 과정이 필요하다. 휴대폰 메모리 데이터 획득을 위해서는, 상용 포렌식 소프트웨어 툴을 이용하는 방법, JTAG-debugging test access port를 이용한 접근방법, 메모리 칩 분리에 의한 물리적 접근방법이 있다.
본 논문에서는 JTAG 인터페이스를 이용하여 CPU 칩을 제어하여 휴대폰 메모리에 접근한다. 이를 통해 메모리 데이터 읽기가 가능해 휴대폰 포렌식의 방법이 된다. PCB로부터 JTAG 시그널을 찾아 직접 연결하거나 표준 24핀 인터페이스로 연결된 신호를 찾을수도 있다. 하지만, 대부분의 휴대폰 제조업체는 핀 구성도나 이와 관련된 정보를 공개하지 않는다. 24핀 연결의 경우 양산품에서 JTAG 단자를 끊는 경우가 대부분이고, 최근 출시된 폰의 경우 JTAG 단자 찾기가 매우 어렵다. 그림 3은 여러가지 방법으로 몇가지 타겟 폰과 JTAG 디버거와 연결한 것이다.

그림 1. 타켓폰의 JTAG 인터페이스 연결

휴대폰 데이터 획득에서 JTAG 인터페이스를 사용하는 가장 큰 장점은 메모리 칩의 de-soldering 없이 플래쉬 메모리에 엑세스 할수 있다는 것과 완전한 포렌식 이미지를 획득할 수 있다는 것이다. 이는 forensically sound한 특성을 만족한다.

Ⅲ. JTAG을 이용한 휴대폰 데이터 수집

그림 2와 같이 구성하여 휴대폰 메모리 획득을 위해서는 다음과 같은 순서를 따른다.

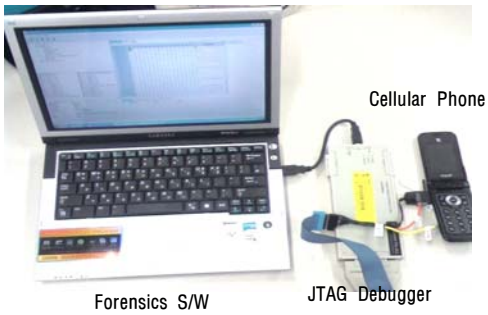

그림 2. JTAG을 사용한 메모리 데이터 획득 장치

1) 휴대폰의 JTAG 핀 찾기
PCB에서 TDI, TDO 등의 JTAG 신호를 찾아서 PCB로부터 직접 배선을 하여 휴대폰 포트와 연결하는 케이블을 제작한다.
2) JTAG 디버깅 환경 설정
Treace32, ICE 등의 JTAG 디버거 장비를 대상이 되는 휴대폰 칩셋에 맞게 세팅한다. 타겟의 기준 전압을 디버거로 인가하여 환경설정이 성공적임을 확인한다.
3) 메모리 바이너리 데이터 획득
읽고자 하는 시작주소와 획득할 크기를 정하여 칩셋과 메모리의 데이터시트를 참고하여 플래쉬 메모리로부터 데이터를 덤프한다.

JTAG을 이용한 메모리 데이터 추출 방식의 장점은 첫째, 기존의 소프트웨어 포렌식 툴과는 달리 휴대폰 전용 드라이버와 케이블의 불필요하고 물리적으로 메모리 전체 영역 수집이 가능하다. 그래서, 파일시스템 영역뿐 아니라 코드영역과 모든 블록을 추출함으로서 폰 사용자가 의도적으로 숨겨놓은 데이터까지 발견이 가능하다. 둘째, 데이터가 기록된 영역이 overwrite 되지만 않았다면 삭제된 데이터(SMS, 전호번호부, 통화목록, 사진 등)에 대해서도 복구가 가능하다. 셋째, 하나의 폰에 대해 데이터를 한번만 획득하면 추후에 포렌식 조사를 위해 다시 데이터를 획득할 필요가 없다. 원본과 복사본의 해쉬값을 비교함으로써 복사본의 무결성을 검증할수 있다.
그림 3은 상기와 같은 방법으로 획득한 메모리 데이터를 보여주는 새로운 포렌식 툴이다.

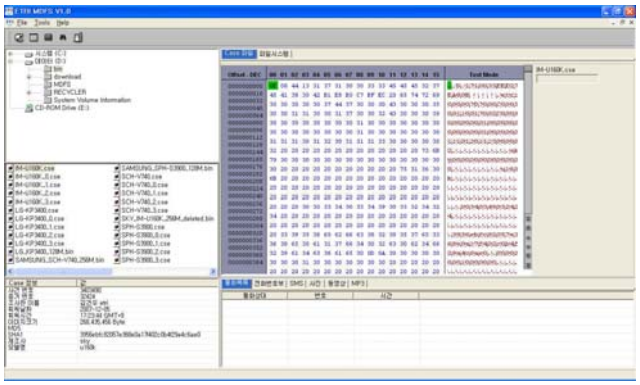

그림 3. 획득된 메모리 데이터

Ⅳ. 결론 및 향후 연구 방향

기존의 상용 모바일 포렌식 툴은 소프트웨어 접근방식을 이용하므로 파일시스템 이외의 영역으로부터 데이터 추출은 한계가 있어 메모리 내용의 100% 추출이 어렵다. 그래서, 본 논문에서는 소프트웨어 툴을 이용하여 데이터 추출이 불완전한 경우, Low-level 접근법인 JTAG 인터페이스를 사용하여 낸드 플래쉬 메모리 전체영역의 데이터를 수집하였다.
향후 정상적으로 파일을 복원한 후 해당 파일을 의미있는 데이터로 변환하는 디코딩 과정이 좀더 개발되어야 한다. 또한, 추출한 증거 데이터와 분석 결과를 법적 효력이 있는 자료로 사용하기 위한 보고서 작성 기능이 추가되어야 한다.

참고문헌

[1] Marcel B. 외, Forensic Data Recovery from Flash Memory. Small Scale Digital Device Forensics Journal, Vol. 1, No. 1, June 2007.
[2] M. F. Breeuwsma, Forensic imaging of embedded systems using JTAG (boundary-scan). Digital Investigation, Vol. 3, Ed. 1, March 2006.
[3] W. Jansen외, Guidelines on Cell Phone Forensics, NIST Special Publication 800-101, May, 2007.

본 연구는 정보통신부 및 정보통신연구진흥원의 IT신성장동력핵심기술개발사업의 일환으로 수행하였음. [2007-S019-01, 정보투명성 보장형 디지털 포렌식 시스템 개발]