갤럭시 스마트폰의 데이터 분석 및 추출 방법

조영호 황지민 ○ 조진성

경희대학교 컴퓨터공학과
namespace@khu.ac.kr jim1286@khu.ac.kr chojs@khu.ac.kr

How to analyze and extract data from Samsung Galaxy smartphones

Youngho Jo Jimin Hwang ○ JinSung Cho

Department of Computer Science and Engineering, KyungHee University

요 약

스마트폰은 현재 삶의 필수품이라고 볼 수 있을 정도로 많은 사람들의 소유물이 되었다. 다만 이러한 스마트폰은 개인정보를 가장 많이 닮고 있는 도구이며 이 때문에 범죄의 표적이 되기도 한다. 디지털 포렌식을 위한 갤럭시 스마트폰에 대한 데이터분석 및 수집을 진행하여 추후 이루어질 갤럭시 스마트폰 포렌식의 기초 데이터를 만들고, 결론적으로 안드로이드 운영체제에서 데이터를 수집, 분석하는 포렌식 도구를 개발하는 것이 최종 목표이다.

1. 서 론

스마트폰이 등장하고 나서 스마트폰은 개인 정보를 가장 많이 담고 있는 도구가 되었고 이 때문에 범죄의 표적이 되기도 한다. 이와 반대로 범죄 활동을 증명하는 수단으로 스마트폰을 분석하는 기술 중에 하나인 디지털 포렌식 기술이 활용되고 있다. 그 역할을 해줄 수 있게 해주는 기술을 디지털 포렌식이라고 한다. 디지털 포렌식은 디지털 증거물을 분석하여 수사에 활용하고, 디지털 증거물의 증거 능력을 향상하기 위한 과학 수사 기법을 총칭하는 용어이다. 포렌식 기술은 앞으로 점점 스마트폰을 이용한 범죄에 필수적인 기술로 자리 잡을 예정이며, 더 많은 연구가 요구되고 있다.

포렌식 도구의 개발에 대한 요구는 꾸준히 늘고 있으며, 데이터를 복구하기 위해서는 연구가 필요하다고 판단이 되었다. 따라서 안드로이드 운영체제에서 데이터를 수집, 분석하는 포렌식 도구를 개발하려고 한다.

본 논문에서는 대표적인 스마트폰인 안드로이드 갤럭시를 대상의 디지털 포렌식 기술을 제안한다. 제안하는 기술은 안드로이드 장치와 통신하게 해주는 ADB 툴과 안드로이드 내부 데이터에 접근 가능하게 해주는 루팅이다.

2. 기존 연구

2.1 ADB

안드로이드 장치와 통신하여 디버깅 등의 작업을 진행할 수 있는 Commend line tool 안드로이드 SDK에도 포함되어 있으며 애플리케이션 설치, 디바이스 접속 및 관리, 파일 앱/다운로드, 시스템 log 출력, shell 접속 등이 가능하다. 따라서 접근이 제한되어 있는 애플리케이션의 데이터에 대해 복원, 추출이 가능하다.

[그림 1], [그림 2]는 ADB 툴을 통해 추출한 데이터 파일이다.

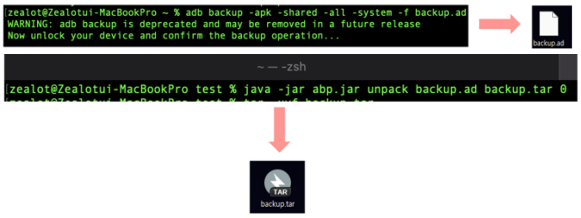

그림 1 ADB backup 명령어 활용

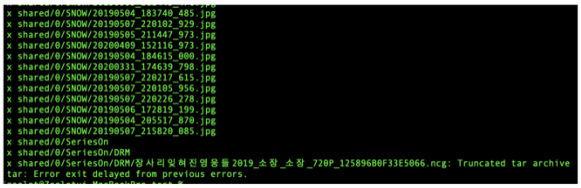

그림 2 Tar 파일 압축해제 후 분석

2.2 루팅

루팅은 모바일 기기에서 구동되는 안드로이드 운영 체제 상에서 최상위 권한을 얻음으로 해당 기기의 생산자 또는 판매자 측에서 걸어 놓은 제약을 해제하는 행위를 가리키는 말이다.

이 루팅을 통해서 데이터에 접근이 가능해지기 때문에 갤럭시 폰에 대한 루팅이 필요하다.

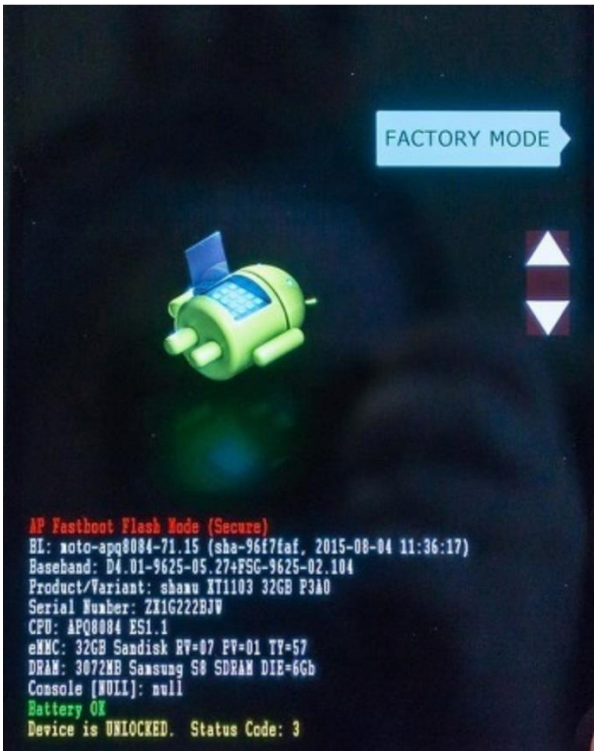

그림 3 안드로이드 루팅

3. 문제 정의

루팅을 하지 않은 핸드폰에 대해 접근할 수 있는 파일 시스템에 한계점이 있다. 가장 개인정보가 많이 저장되어 있는 시스템에 접근하기 위해선 권한이 부족한 상태이다.

항 목	파일 경로
커널 정보	/data/log/recovery_kernel_log.txt
리커버리 로그	/data/log/recovery_log.txt
전원 종료 로그	/data/log/poweroff_info.txt
전원 재시작 로그	/data/log/powerreset_info.txt
전원 부팅 로그	/data/log/rtc.log
통화중 단절 로그	/data/log/CallDropInfoLog.txt
앱 에러 로그	/data/log/dumpstate_app_error.txt.gz
공유기 연결 로그	/data/misc/wifi/wpa_supplicant.conf
블루투스 정보	/data/misc/bluetoothd/config
앱 실행 정보	/data/system/dmappmgr.db
설치된 앱 정보	/data/system/packages.xml
등록된 계정 정보	/data/system/users/0/accounts.db
자동 로그인 계정 정보	/data/system/registered_services/android.accounts.AccountAuthenticator.xm
자동 동기화앱 목록	/data/system/registered_services/android.content.SyncAdapter.xml

그림 4 안드로이드 모바일기기의 시스템 데이터

안드로이드 버전이 올라감에 따라 내부 데이터 접근이 더욱 어려워 졌으며, ADB 툴을 이용하여 데이터를 추출하는데 한계가 있다.

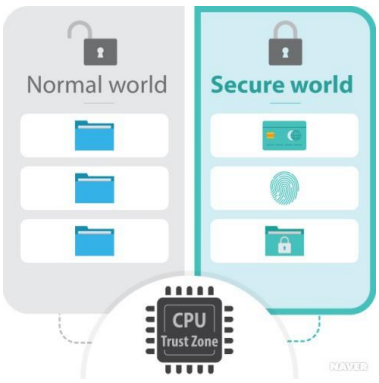

그림 5 내부 데이터 구조

추출한 데이터 파일에 암호화 되어 있는 경우가 있어서 추출하더라도 해독이 필요한 경우가 있다.

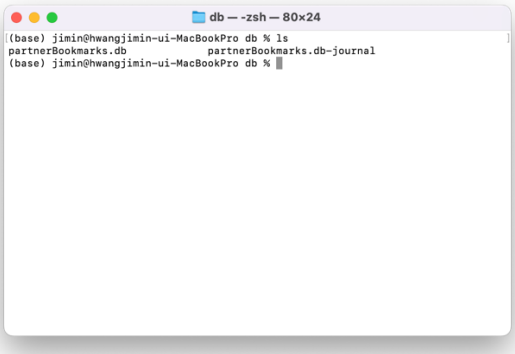

그림 6 추출한 데이터 파일 폴더

그림 7 암호화 되어 있는 파일

4. 토의

현재 정의된 문제는 2가지가 있다. 첫째는 루팅 없이 갤럭시 스마트폰에 접근할 수 있는 데이터는 한정되어 있다는 점이다. 두번째 문제는 ADB를 통해 수집할 수 있는 데이터를 수집해본 결과, 실제 데이터에 접근할 수 없도록 암호화가 되어 있는 파일들이 존재한다는 점이다.

첫번째 문제를 해결하기 위해 여러가지 해결 방안을 고민해볼 수 있다. 루팅을 통해 루트 권한을 획득하는 방법, 물리적으로 메모리를 추출하여 파일시스템에 접근하는 방법, Smart Switch(삼성 스마트폰 백업 프로그램)의 데이터를 하이재킹하여 데이터를 수집하는 방법 등을 제시할 수 있다.

루팅을 통해 루트 권한을 획득할 경우 가장 쉽게 루트 권한을 취득할 수 있다는 장점이 있다. 다만 안드로이드 버전 업에 따라 루팅을 할 수 있는 커널이 업데이트 될 때까지 기다려야 한다는 단점이 있으며, 또한 추후 포렌식 진행 시 데이터의 무결성에 문제가 생길 수도 있다.

두번째로 물리적으로 메모리를 추출하여 파일시스템에 접근하는 방법은 추가 작업이 필요없이 메모리를 추출하면 되기 때문에 시간적으로 가장 빠르다는 장점이 있다. 다만 PUF(Physical Unclonable Function)이 적용되어 있는 갤럭시 스마트폰의 경우 물리적인 추출을 진행할 경우 데이터가 모두 손상될 수 있다는 단점이 있다.

마지막으로 Smart Switch(삼성 스마트폰 백업 프로그램)의 데이터를 하이재킹 할 경우, 물리적, 논리적 손상 없이 데이터를 추출할 수 있다는 장점이 있다. 다만 실제로 하이재킹을 위한 연구를 추가 진행해야 한다는 단점이 있다.

표 1. 스마트폰 데이터 접근 방안별 장단점

방안	장점	단점
루팅	쉽게 루트권한 취득 가능	추후 진행 연구의 데이터 무결성 위협
물리적 추출	시간적으로 가장 빠르며, 쉽게 파일시스템 접근 가능	PUF의 존재 유무에 따라 데이터 손상 가능
Smart Switch	물리적, 논리적 손상 없이 데이터 추출 가능	추가 연구 필요

두번째 문제를 해결하기 위해 분석 대상 스마트폰을 추가 분석하여 실제로 얻어낼 수 있는 데이터들을 파악할 수 있다. 예를 들면 기본 인터넷 브라우저의 즐겨찾기 등의 사용자가 쉽게 접근할 수 있는 데이터를 기준으로 암호화되어 있는 데이터에 접근하여 추가 분석을 진행한 뒤 암호화되어 있는 데이터를 복호화 할 수 있다.

5. 결론 및 향후 연구

우선 루팅을 통해 취득할 수 있는 모든 데이터를 취득한 뒤, ADB 등 추가 작업 없이 접근할 수 있는 데이터와 비교 대조할 예정이다. 이를 통해 추가작업이 필요한 데이터와 필요하지 않은 데이터를 나누고, 루팅을 하지 않고도 얻은 데이터에서 유추가 가능한지에 대한 연구를 진행할 것이다.

마지막으로 실제 포렌식을 위해서는 삭제되어 있는 파일 혹은 암호화되어 있는 파일을 분석하여 제공할 필요가 있다. 이를 위해 파일 시스템 전체를 이미지화하여 분석할 필요가 있다. 이를 기반으로 안드로이드 운영체제의 삭제파일 카빙 기법연구가 이어져 진행되어야 한다. 이러한 모든 과정은 안드로이드의 버전에 따라, 핸드폰의 보안 수준에 따라 달라질 수 있지만, 갤럭시 스마트폰 뿐만 아닌 다른 스마트폰에 적용하는 등 여러가지 경험을 쌓다보면 추후 진행될 다른 포렌식 연구에 기반이 될 수 있을 것이다.

참고 문헌

[1] 방승규,전상준,김도현,이상진. (2016). HFS+ 저널 파일 파싱 알고리즘을 이용한 삭제된 파일 복구 기법 향상 방안. 정보처리학회논문지 p.463~p.470

[2] 김도현,박정흠,이상진. (2013). 안드로이드 운영체제의 Ext4 파일 시스템에서 삭제 파일 카빙 기법. 한국정보보호학회논문지 제23권 제3호

[3] 김도현, 이상진. (2016). 모바일 포렌식 동향. 한국정보보호학회논문지 제26권 제5호