**Smartphone Mobile Forensic Tool Development**

팀원 : 2016104113 김예미, 2016104137 유희정, 2016104149 이윤영

**개 요**

스마트폰은 대부분의 사람들이 휴대하는 모바일 기기로, 사용자의 다양한 흔적 데이터를 가지고 있어 데이터 수집, 분석을 통해 사용자에 대한 유의미한 정보를 얻을 수 있다. 본 연구에서는 ‘안드로이드 스마트폰 정보 추출방법에 관한 연구’를 기반으로 안드로이드 기반 스마트폰에서 api를 이용해 데이터를 추출하고, 추출한 데이터를 분석, 시각화 할 수 있는 Smartphone Mobile Forensic Tool을 제안하고 구현한다.

1. **서론** 
   1. **연구 배경**

일상의 다양한 정보들이 매 순간 스마트폰과 같은 모바일 디바이스와 여러 주변 기기를 통해 데이터로 기록된다. 이 데이터들은 그 자체로도 유의미하지만, 다량의 데이터를 해석하고 분석해 다양한 분야에 활용할 수 있다.

특히 많은 범죄수사에서 증거 수집을 위해 디지털 포렌식을 이용해 디지털 장비의 데이터를 수집/분석한다. 최근 늘어나는 사이버 범죄에서도 스마트폰 기기의 데이터가 범죄수사의 증거로서 중요한 역할을 하고 있다.

모바일 포렌식 툴 개발은 데이터 수집과 데이터 분석의 과정으로 구성된다. 앞서 ‘안드로이드 스마트폰 정보 추출방법에 관한 연구’에서 데이터 추출에 관한 연구를 완료했으며, 이 연구를 기반으로 실제 디지털 포렌식 도구를 개발하고자 한다.

본 연구에서는 데이터를 복구 수집해 데이터 자체가 가진 의미에 집중하는 기존의 포렌식 도구에서 나아가 새로운 관점으로 데이터를 바라보고 6가지 주제를 설정하여 데이터를 분석한다.

* 1. **연구목표**

상용되는 모바일 포렌식 도구는 루팅된 스마트폰을 기본조건으로 한다. 하지만 최신 기종 스마트폰의 루팅이 더욱 어려워지고 있으며 스마트폰 어플리케이션 자체에서도 데이터를 암호화해 저장하는 경우가 늘어나고 있어 스마트폰 데이터에 대한 접근과 활용에 제약이 있다.

이에 본 연구는 루팅하지 않은 안드로이드 스마트폰을 대상으로 모바일 포렌식 툴 개발을 진행한다. 안드로이드 api를 통해 획득 가능한 제한된 범위의 스마트폰 데이터를 추출하여 분석한다.

데이터의 단편적인 해석에서 벗어나 다양한 시점에서 분석해 흥미로운 결과를 제시한다. 데이터 분석 결과는 그 의미를 부각시킬 수 있는 다양한 방법으로 시각화 한다.

데이터 추출용 안드로이드 모바일 앱을 구현해 데이터를 추출하고 포렌식 프로그램에 전송한다. 모바일 어플리케이션에서의 데이터 추출과 PC 포렌식 프로그램으로의 전송 및 저장 과정을 모두 자동화한다.

1. **기존 연구**
   1. **모바일 포렌식 증거 수집방안 연구: 제조사 백업 앱 기반 데이터 획득 기법**

제조사에서 기본으로 제공하는 백업용 모바일 앱을 이용하여, 최근 보안이 강화되어 기존 데이터 획득 방법을 그대로 적용하기 어려운 안드로이드 스마트폰에서의 데이터 획득 과정을 다룬다.

2007년부터 2017년까지 국내에 출시된 21개 제조사의 1,850대의 폰을 대상으로 기존 데이터 획득 기법의 적용 가능 여부를 조사한 결과, 기존의 하드웨어 기반의 Chip Off, JTAG 방식과 소프트웨어 기반의 Custom Image, Bootloader기반의 데이터 획득 기법은 2017년 출시된 폰을 대상으로는 더 이상 적용 가능하지 않음을 확인하였다. 기존의 데이터 획득 기법은 폰의 취약점에 기반한 기법이기 때문에 공개된 이후 패치와 업데이터를 통해 해당 취약점은 제거되는 과정을 거치게 되고, 이에 따라 최초 데이터 획득 기법이 소개된 이후 시간이 경과할수록 적용 가능한 폰이 감소한다.

스마트폰 제조사들은 다양한 백업용 모바일 앱을 사용자에게 기본으로 제공한다. 이들은 스마트폰의 플래시 메모리에 저장된 사용자 데이터를 백업하고 복원하는 기능을 기본으로 제공하며, 일반 사용자 권한으로는 접근이 불가능한 데이터를 포함하여 백업한다. 백업 앱 실행 및 대상 데이터 선택, 백업파일 생성, 수신용 폰으로 생성파일 전송, 백업 파일 전송 및 복호화, 압축 해제 후 데이터 복원의 과정을 거쳐 사용자의 데이터가 백업되고 복원되는데 데이터 획득 대상 스마트폰에서 수신용 스마트폰으로 데이터가 전송되는 과정에서 임시 생성된 파일을 중간에 가로채는 방식으로 사용자 데이터 획득이 가능하다.

연락처, 메시지, 일정 등 DB형태로 저장되는 파일은 암호화가 적용된 상태로 전송되며, 이미지, 동영상, 음성녹음, 문서 등 멀티미디어 파일은 기존 획득 대상 스마트폰과 동일한 경로에 파일이 복사된다.

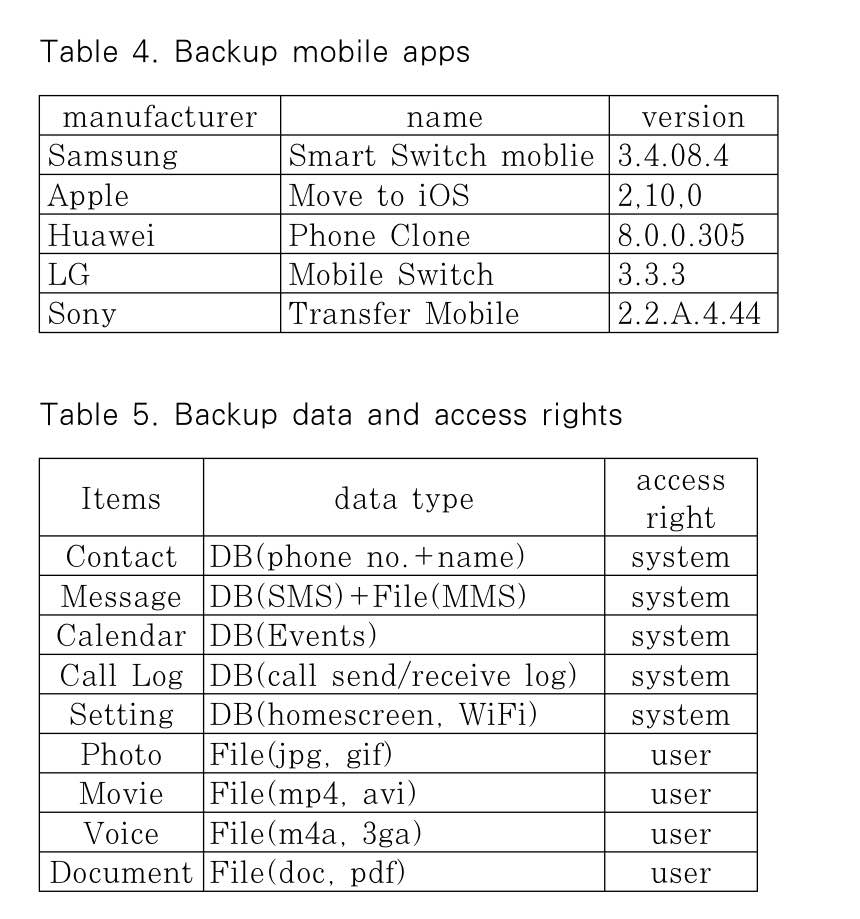


그림 1) 스마트폰 제조사들이 제공하는 백업 앱과 백업 가능한 주요 데이터 항목

* 1. **패스워드 매니저 취약점을 이용한 사용자 계정 탈취 방법**

패스워드 매니저는 사용자 계정 정보를 관리해 줌으로써 사용자에게 관리의 편리함과 취약한 아이디와 패스워드에 대해 보안성을 제공한다. 패스워드 매니저 소프트웨어는 하드드라이브에 설치하는 소프트웨어이며 사용자 아이디와 패스워드를 해당 컴퓨터 및 스마트폰에 저장한다. 하지만 공격자가 해당 기기의 데이터베이스에 접근이 가능 하거나, 마스터 암호를 알고 있다면 사용자의 모든 인터넷 서비스의 계정 정보를 위협할 수 있다는 취약점이 존재한다.

가령 루팅이 가능한 안드로이드 스마트폰 환경에서 패스워드 매니저를 사용하는 Chrome 브라우저는 암호화된 패스워드를 특정 경로의 데이터베이스에 저장하며, 공격자가 마스터 암호를 알지 못하더라도 데이터베이스에 접근하여 저장된 모든 계정 정보를 탈취할 수 있다. 패스워드 매니저를 관리하는 LastPass 어플리케이션의 경우, 마스터 암호가 저장되어 있는 저장소에 접근이 가능하다면 공격자는 이를 우회 로그인하여 모든 계정 정보를 탈취할 수 있다.

이러한 계정 정보 유출 및 우회 로그인에 대한 대응 방안으로 사용자 계정 정보가 저장되어 있는 패스워드 매니저 파일에 접근 권한 설정, 사용자의 계정 정보 암호화, 잠금 화면을 설정하고 해제할 수 있는 기능 제거를 제시한다.

* 1. **기존 연구의 문제점**

2.1 연구의 경우 특정 제조사를 한정하여 해당 제조사에서 생산한 스마트폰에만 범용적으로 적용 가능한 데이터 획득 기법을 연구하였기 때문에 안드로이드를 사용하는 모든 스마트폰에 범용적으로 적용이 가능한 데이터 획득 기법에 대한 연구가 향후 과제로 남아있다는 한계가 있다.

2.2 연구의 경우 루팅이 가능한 안드로이드 스마트폰 환경을 전제로 하며, 사용자 계정 정보 데이터 획득 방법 및 대응 방안에 초점을 맞추어 진행된 연구로 스마트폰에서 추출 가능한 모든 사용자 흔적 데이터를 다루지 않는다는 한계가 있다.

1. **프로젝트** 
   1. **기존 연구와 차이점 및 해결방안**

위에 언급한 두 기존 연구는 루팅이 가능한 안드로이드 스마트폰 혹은 특정 제조사에서 생산한 스마트폰 환경을 전제로 하여 안드로이드 스마트폰에 범용적으로 적용이 어렵다. 특정 데이터 획득 방법 및 취약점 분석에 초점을 맞추어 진행된 연구로, 포렌식 툴 개발과는 방향성이 다르다.

이외에도 최근 연구의 대부분이 특정 앱의 디지털 포렌식에 대한 연구이거나 암호화 및 복호화에 관련된 논문이며, target device 데이터를 루팅이 된 intermediate device로 이동하여 디지털 포렌식을 진행하는 등 새로운 연구의 경우 유효성과 적용 가능 기종, 수집 데이터의 범위 등에 대해 제한된 연구가 진행되고 있다.

본 프로젝트는 루팅되지 않은 안드로이드 스마트폰 환경을 대상으로 Content Provider를 통해 사용자 흔적 데이터를 획득하고, 획득한 데이터를 분석하여 다양한 정보를 제공하는 모바일 포렌식 툴을 개발한다.

* 1. **프로젝트 내용**

데이터 추출을 위한 안드로이드 앱과 추출된 데이터를 표현하는 데스크톱 앱의 형태로 구성한다. 안드로이드 앱에서 데이터를 추출하여 DB에 저장하고 PC에서 이를 백업하여 DB파일을 획득, 분석한다.

**3.2.1 데이터 추출**

안드로이드 api를 이용해 추출 가능한 데이터 중 본 연구에서 추출할 데이터는 다음과 같다.

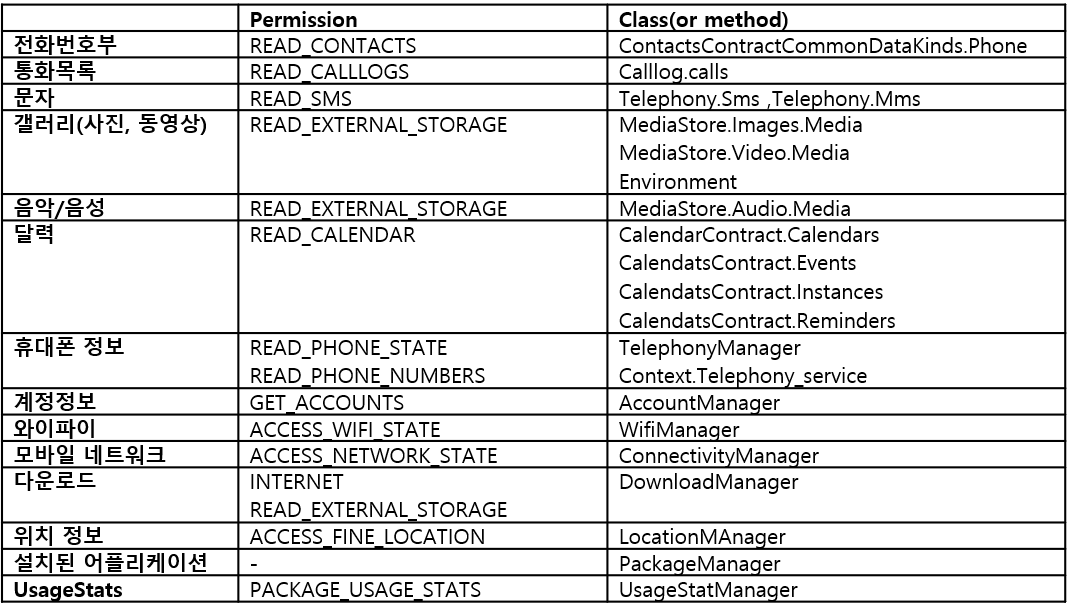
****

그림 2) 안드로이드 ap를 통해 추출할 데이터와 관련 권한과 클래스 및 메소드

데이터 추출 앱에서 데이터를 추출해 DB에 저장한다. 저장된 DB를 PC 프로그램에서 백업하고 분석을 이어간다. 데이터 추출, 저장 및 백업 과정은 모두 자동화한다.

**3.2.2 데이터 분석**

획득한 사용자 데이터를 아래의 6가지 주제로 분석하여 표현한다.

**3.2.2.1 연락처, 문자, 통화기록 분석**

연락처, 통화 및 문자 기록을 분석하여 사용자의 연락 패턴을 분석한다.

1. 전체 분석을 통한 인사이트 제공

누적 통화 및 문자 건수, 누적 통화 시간에 대한 통계를 그래프로 제공한다.

1. 목록 분석

전체 통화 및 문자 목록을 시간순으로 출력한다. 특정 날짜 및 기간의 목록 출력, 수신·발신·부재중과 통화·문자로 구분하여 출력, 특정 연락처와의 연락 목록 출력의 상세 목록 분석 결과를 제공한다.

1. 상세 분석

특정 기간의 연락 건수, 통화 시간 통계, 연락 빈도 순위, 선호 연락 시간대, 평균 문자 답장 시간 등 추가적인 분석 결과를 제공한다.

**3.2.2.2 문자 키워드 분석, 결제문자 분석**

전체 문자 혹은 특정 상대와의 문자 기록에 대해 자연어 처리를 통해 자주 언급되는 키워드를 분석한다.

특히 은행에서 제공하는 sms 결제 알림 문자 서비스에 의해 발생하는 문자 기록은 지출 금액 및 날짜, 사용처 정보를 포함하고 있으며 은행마다 제공하는 문자 형식이 다르므로 추가적으로 분석하여 사용자 소비 패턴을 분석한다.

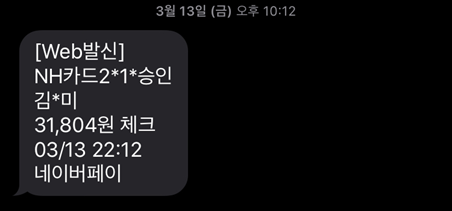


그림 2) 농협 결제 알림 문자 형식

**3.2.2.3 어플 관련 분석**

어플 목록, 설치된 날짜, 마지막 사용 시간, 실행 시간, 사용 횟수, 네트워크 사용량을 분석한다.

1. 전체 분석

실행시간, 사용 횟수 등의 비율을 파이그래프로 제공하면서 사용자가 핸드폰 이용자의 어플 사용에 대한 전체적인 확인이 쉽도록 한다.

마지막 사용 시간을 타임라인으로 제공한다.

1. 목록 분석

설치된 어플의 목록을 리스트로 제공한다. 사용시간, 실행 시간, 사용 횟수 등으로 정렬이 가능하고 각각의 어플에 대한 세부 정보를 확인할 수 있도록 출력한다.

1. 특이사항 확인

Google Play Store나 One store 등 정상적인 경로 이외에 다른 경로로 설치한 어플리케이션의 목록과 특이사항을 제공한다.

**3.2.2.4 다운로드 파일 분석**

내장 메모리 내의 다운로드 파일들을 분석한다.

1. 전체 분석

내장 메모리 내의 다운로드 파일들의 종류와 비율을 분석하여 그래프로 제공한다. 시간대별 다운로드 패턴도 분석하여 보여준다.

1. 출처 분석

출처가 존재하는 다운로드 파일의 출처를 표시하고 비슷한 출처에 따라 분류한다.

1. 검색

특정 기간동안 다운로드된 파일을 검색할 수 있도록 검색 기능을 제공한다.

**3.2.2.5 사진 분석 및 분류**

사진의 날짜, 위치 데이터를 이용해 분류 및 검색기능을 제공하고 머신러닝을 이용해 사진을 분석해 사진의 종류를 분류한다.

1. 날짜를 이용한 분류

사진이 찍힌 날짜 혹은 저장된 날짜를 이용해 선택한 날짜 및 기간에 해당하는 사진에 대한 검색기능을 제공하고 분류한다.

1. 사진 위치를 이용한 분류

사용자가 촬영한 사진에 한해 존재하는 사진의 위치 데이터를 이용해 사진의 위치를 마크한 지도를 제공한다. 비슷한 위치에서 찍은 사진끼리 분류가 가능하다.

1. 머신러닝을 이용한 사진 분류

머신러닝 또는 딥러닝을 이용해 사진을 자연, 인물, 동물, 음식 등의 레이블로 분류하고 레이블 별로 확인이 가능하다.

**3.2.2.6 사용자 타임라인 분석**

앱 사용시간, 통화시작, 종료, 및 지속시간, 문자 발신 및 수신 시간, 사진 촬영 시간 등 모든 시간 데이터를 이용해 사용자 타임라인을 만든다.

날짜를 선택하면 사용자의 시간대 별 행동을 확인할 수 있다. 이를 시간대 별로 하루의 타임라인을 확인할 수 있도록 시각적으로 제시하며, 사용자가 직접 행동에 대한 코멘트를 추가하여 파일로 저장 가능하도록 한다.

1. **진행 일정 및 역할 분담**

|  |  |  |
| --- | --- | --- |
| **진행 주차** | **담당** | **내용** |
| ~4 | 전원 | 프로젝트 관련 자료 수집 및 설계, 계획서 작성 |
| 5~6 | 전원 | 안드로이드 기반 기기 데이터 추출 및 확인 |
| 7~8 | 전원 | 데이터 추출 및 전송용 안드로이드 앱 개발 |
| 9 | 전원 | 데스크톱 앱의 데이터 수신 기능 개발 |
| 10~11 | 이윤영 | 전체 추출 데이터 목록 출력 기능 개발 |
| 10~13 | 김예미 | 연락처, 문자, 통화기록 분석 기능 개발 |
| 10~13 | 김예미 | 문자 키워드 분석, 결제문자 분석 기능 개발 |
| 10~13 | 이윤영 | 어플 목록, 사용기록 관련 분석 기능 개발 |
| 10~13 | 이윤영 | 다운로드 파일 분석 기능 개발 |
| 10~13 | 유희정 | 사진 분류 기능 개발 |
| 10~13 | 유희정 | 사용자 타임라인 기능 개발 |
| 13~14 | 전원 | 디버깅 |
| 15 | 전원 | 발표, 최종보고서 정리 |

1. **결론**

스마트폰에 존재하는 데이터를 추출 및 분석하는 도구를 만든다. 이 프로그램의 데이터 추출방법은 논리적 추출의 안드로이드 api (Content provider)를 이용하는 방법이다. 무결성의 보장이 어렵다는 점 때문에 대부분의 모바일 포렌식 도구가 Rooting kernel이나 물리적 데이터 수집을 사용하였으나 안드로이드의 버전 업데이트와 새로운 기기의 출시에 따른 보안성 향상으로 기존 데이터 수집 방법의 적용 범위가 줄어들고 있다. 이런 상황에서 안드로이드 api를 통한 추출을 기반으로 한 디지털 포렌식 도구는 새로 출시되는 기기부터 예전 기기까지 다양한 안드로이드 기기에 대한 보편적인 분석 방법을 제공할 수 있다.

본 프로그램은 안드로이드 기반 스마트폰에서 추출할 수 있는 데이터와 그 목록을 제공하고, 6가지 주제로 세부 분석한 결과를 시각화하여 보여준다. 데이터의 나열만이 아니라 시각화된 정보도 제공하기 때문에 사용자가 데이터 해석을 할 때 시간적인 측면에서 도움을 줄 수 있다.

**참고 문헌**

[1] 최재원, 김승주, 모바일 포렌식 증거 수집방안 연구 제조사 백업 앱 기반 데이터 획득 기법, 정보보호학회논문지, 28(1), 95-110, 2018.2

[2] 남기훈, 석병진, 공성현, 김역, 이창훈, 패스워드 매니저 취약점을 이용한 사용자 계정 탈취 방법, 디지털 포렌식 연구, 12(1), 9-18, 2018.6

[3] 서승희, 박진성, 김 역, 이창훈, 디지털 포렌식 측면에서의 안드로이드 디바이스에 대한 데이터 추집 연구, OSIA Standards &amp; Technology Review, 31(2), 12-17, 2018.