|  |
| --- |
| **안드로이드 스마트폰 모바일 포렌식 도구** |
|  |
| **Android Smartphone Mobile Forensic Tool** |
|  |
| **요 약**  스마트폰은 사용자가 24시간 휴대하는 모바일 기기로 통화기록, 문자기록, 앱 사용기록, 사진, 비디오 등 다양한 흔적 데이터를 가진다. 이러한 데이터를 수집 및 분석하여 사용자에 대한 유의미한 정보를 얻을 수 있다. 본 연구는 루팅하지 않은 안드로이드 기반 스마트폰을 대상으로 포렌식을 수행하는 데스크톱 앱 형태의 Smartphone Mobile Forensic Tool을 제안한다. 안드로이드 애플리케이션에서 API를 이용해 데이터를 추출하고, PC 포렌식 프로그램에서 획득한 데이터를 통합, 6가지 주제로 분석하여 시각화 하도록 구성한다. |

**1. 서 론**

최근 사이버 범죄가 증가함에 따라 범죄 수사에서는 증거를 수집하기 위해 디지털 장치의 데이터를 수집 및 분석하는 이른바 디지털 포렌식 기법을 활용한다. 특히 사진, 비디오 등 미디어 데이터부터 통화·문자·앱 사용 기록에 이르는 일상의 다양한 정보들이 매 순간 모바일 기기를 통해 데이터로 기록되므로 스마트폰 기기의 데이터의 분석이 범죄 수사의 증거로서 중요한 역할을 차지하고 있다.

상용되는 모바일 포렌식 도구는 기기에 대한 최고 권한을 획득하는 ‘루팅’을 기본조건으로 한다. 하지만 최신 기종 스마트폰의 경우 ‘루팅’을 통한 데이터 획득이 어려워지고 있으며, 애플리케이션 자체에서 데이터를 암호화해 저장하는 경우가 늘어나고 있어 기기 데이터에 대한 접근과 활용에 제약이 있다. 이에 본 연구는 루팅하지 않은 안드로이드 스마트폰을 대상으로 모바일 포렌식을 수행하는 도구 개발을 진행한다.

본 연구에서 제안하는 모바일 포렌식 도구의 수행은 데이터 추출·분석·출력의 과정으로 이루어진다. 앞서 ‘안드로이드 스마트폰 정보 추출 방법에 관한 연구’에서 데이터 추출에 관한 연구를 완료했으며, 제시한 4가지 방법 중 안드로이드 API를 통해 데이터를 획득하는 방법과 adb 백업 방법을 사용한다. 6가지 주제를 설정하여 획득한 데이터를 통합적으로 분석한다. 분석 결과는 그 의미를 부각할 수 있도록 시각화해 제공한다.

루팅하지 않은 안드로이드 스마트폰을 대상으로 모든 안드로이드 스마트폰에 대하여 보편적으로 동작하는 안드로이드 모바일 포렌식 도구를 개발한다. 사용자 흔적 데이터가 가진 단순한 수치나 값에 집중하는 기존의 포렌식 도구에서 나아가 다량의 데이터를 통합하여 분석하고 이를 시각화 함으로써 데이터를 보다 다양한 분야에 활용할 수 있도록 하는데 의의가 있다.

**2. 관련연구**

**2.1 디지털 포렌식 측면에서의 안드로이드 디바이스에 대한 데이터 추집 연구[1]**

안드로이드 기기의 디지털 포렌식 절차와 데이터 수집 연구들을 정리한다. 논리적 데이터 수집에는 Rooting kernel, Backup Protocol과 Tool, Content Provider, LASM 등이 있고 물리적 데이터 수집에는 Firmware update protocol, JTAG, Chip-off, 클라우드 데이터 수집이 있다. 안드로이드 기기의 다양성과 OS 버전 갱신, 보안성 향상 때문에 기존 데이터 수집 방법의 사용 기기 범위가 줄어들고 있다. Data 파티션 자체를 암호화하여 저장하면서 chip-off 등 물리적 데이터 수집도 어려워지고 있다.

**2.2 안드로이드 스마트폰 포렌식 도구**

안드로이드 스마트폰 포렌식 통합 모델이나 도구에 관한 최근 연구 사례를 찾아보기 어렵고, 최근 연구는 스마트폰 데이터에 대한 전반적인 연구보다 특정주제, 불법촬영물이나 블랙박스 등에 초점을 맞춘 포렌식 도구를 제안하고 있다.

현재 상용되는 모바일 포렌식 도구는 다음과 같다.

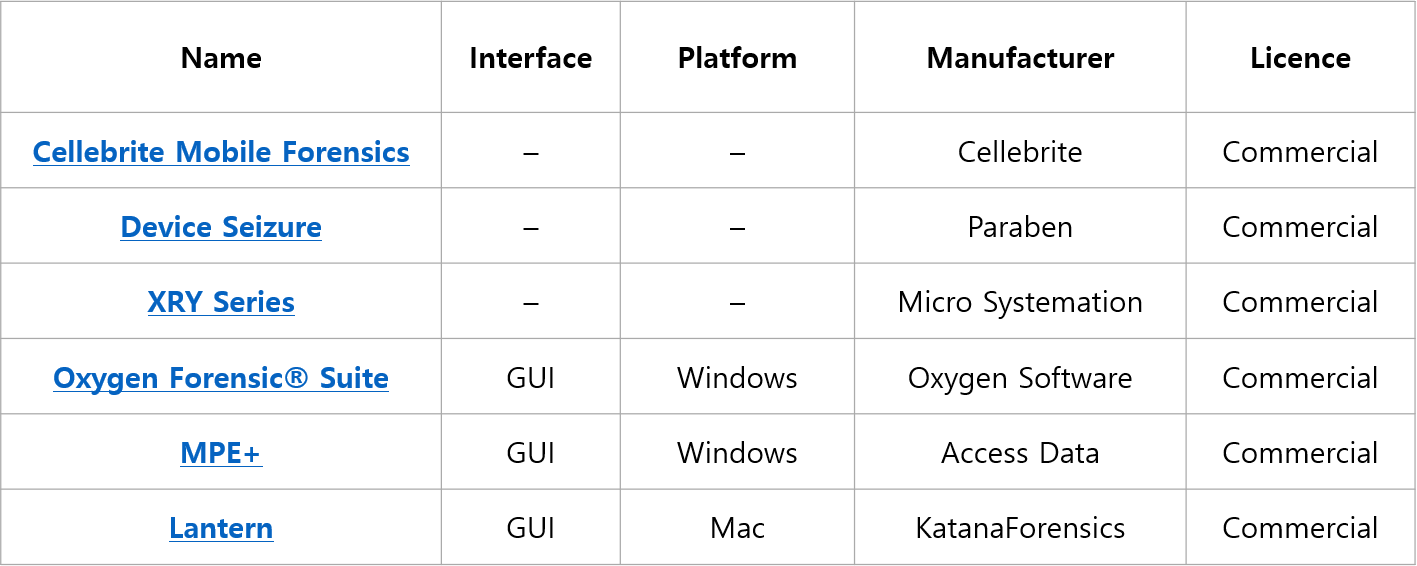


그림 1) 상용 모바일 포렌식 툴

상용되는 포렌식 도구는 대부분 법 집행의 증거, 군사 정보 기밀, 비즈니스 등 공적 목적으로 사용된다. 따라서 개인을 대상으로 한 프로그램이 아니고 포렌식 업체나 전문가를 대상으로 한 프로그램이다. 기본적으로 루팅을 요구하고 논리적 추출에 제한되지 않는다. 물리적 추출과 전체 파일시스템 추출, 디스크 이미징을 통해 훨씬 많은 데이터를 얻을 수 있다. 암호화된 장치의 백업 및 이미징 비밀번호를 찾아내고, 스크린 잠금화면은 우회할 수 있다. 3rd party 앱으로의 접근이 가능하고, 채팅 대화 데이터 획득, 삭제된 콘텐츠 복구가 가능하다.

**3. 제안하는 포렌식 도구**

데이터 추출을 위한 안드로이드 애플리케이션과 추출된 데이터를 분석 및 표현하는 데스크톱 앱의 형태로 구성한다. 안드로이드 애플리케이션에서 데이터를 추출해 데이터베이스에 저장하고, PC에서 이를 백업하여 데이터베이스 파일을 획득, 분석한다.

**3.1 데이터 추출**

 앞서 진행한 ‘안드로이드 스마트폰 정보 추출 방법에 관한 연구’를 기반으로 데이터를 추출한다. 제시한 4가지 방법 중 Content Provider를 통해 데이터를 추출하는 안드로이드 API와 PC에서 기기와 통신할 수 있도록 하는 adb 도구의 backup 기능을 활용한다. API를 통해 추출 가능한 데이터 중 본 연구에서 활용할 데이터는 다음과 같다

표 1) 안드로이드 API를 이용해 추출 가능한 데이터 일부에 대한 관련 권한과 클래스 (또는 메소드)

usb 케이블로 PC에 안드로이드 스마트폰을 연결하고 PC 프로그램을 실행하면 연결된 기기 중 포렌식을 진행할 기기를 선택한다. 해당 기기에 안드로이드 애플리케이션을 설치·실행해 데이터를 추출한다. 안드로이드 애플리케이션에서는 사용자 권한을 요청하고 uri와 query 문을 통해 데이터를 요청해 SQLite 데이터베이스에 획득한 데이터를 저장한다. 애플리케이션 내부에 데이터베이스 구성이 완료되면 소켓 통신을 통해 PC 프로그램에 알림을 전달한다. adb 백업 방법을 통해 애플리케이션 내부에 생성된 데이터베이스를 획득하고 분석을 이어간다. 안드로이드 애플리케이션의 설치, 실행 및 백업 과정은 PC 프로그램의 동작으로 편입하여 모두 자동화한다.영수증, 스크린샷이(가) 표시된 사진

자동 생성된 설명

**3.2 데이터 분석**

획득한 데이터는 아래의 6가지 주제로 세부 분석한다.

**3.2.1 사용자 연락 분석**

연락처, 통화기록 및 문자 데이터를 활용하여 스마트폰 사용자의 연락 패턴을 분석한다. 연락처 데이터에 포함된 전화번호를 중심으로 통화기록 및 문자기록 데이터를 통합하여 사용자와 상대방의 상호작용 내역을 획득할 수 있다. 이때 특정 상대방과의 연락뿐만 아니라 전체적인 연락 특성을 분석하여 사용자의 연락 특성을 파악한다.

먼저 시간대별 통화 및 문자 건수, 통화 시간에 대한 전체적인 수치 통계를 제시하여 사용자의 연락 패턴에 대한 인사이트를 제공한다. 또한 시간순으로 정렬된 통화 및 문자 목록을 분석한다. 특정 기간의 목록, 특정 상대방과의 연락 목록 등을 수신/발신/부재중, 통화/문자, 특정 검색어 등 상세검색 조건에 따라 다양하게 확인할 수 있도록 한다. 마지막으로 사용자의 인간관계를 파악할 수 있는 연락 빈도 순위, 통화량 순위와 사용자의 연락 특성을 파악할 수 있는 사용자가 선호하는 연락 시간대, 평균 문자 답장 시간 등 추가적인 분석 결과를 제공한다.

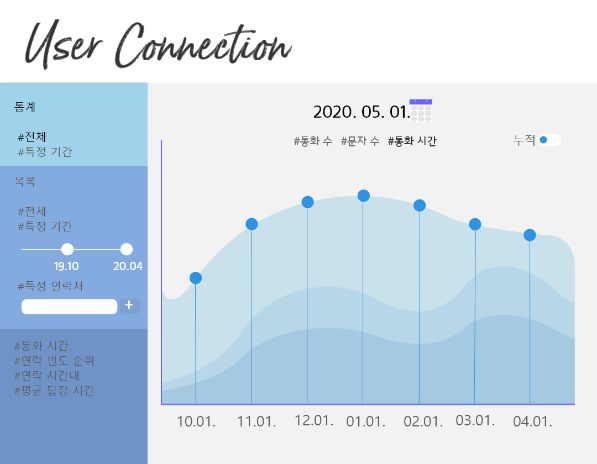


그림 2) 사용자 연락 분석 UI 설계

**3.2.2 문자 키워드 분석**

문자기록의 경우 통화기록과 달리 내용이 스마트폰 기기에 보존되기 때문에 추가적인 분석을 진행한다. 먼저 자연어 처리를 통해 전제 문자, 특정 상대와 주고받은 문자기록에 대해 자주 언급되는 키워드를 분석한다. 특정 상대와 공유하는 주제 및 기기 사용자의 관심사를 파악할 수 있다.

특히 은행에서 제공하는 SMS 결제 알림 문자 서비스에 의해 발생하는 문자기록은 지출 금액 및 날짜, 사용처 정보를 포함하고 있으므로 추가로 사용자의 소비 패턴을 살필 수 있다. 사용자가 주로 소비하는 품목, 지출액 변화 및 지출날짜 변화를 분석하여 사용자의 활동을 파악한다. 다만 은행마다 제공하는 문자 형식이 다르므로 이에 대한 표준화 및 연구가 요구된다.

스크린샷이(가) 표시된 사진

자동 생성된 설명

그림 3) 문자 키워드 분석 UI 설계

**3.2.3 앱 사용 분석**

앱 목록, 설치된 날짜, 마지막 사용 시간, 업데이트 날짜, 실행시간, wifi와 cellular 사용량 등 앱 관련 데이터를 기반으로 앱 사용 분석을 진행한다.

설치된 앱의 목록을 리스트로 제공하여, 사용시간, 실행 시간, 네트워크 사용량 순으로 정렬이 가능하게 하고, 리스트에서 클릭하거나 검색하여 앱에 대한 세부 정보를 확인할 수 있도록 출력한다. 세부 정보에는 기본 정보 이외에도 실행시간 등의 비율을 파이그래프로 제공하면서 사용자가 핸드폰 이용자의 앱 사용에 대한 전체적인 파악이 쉽도록 한다. Google Play Store, One store 그리고 Galaxy Store 등 공인된 경로 외에 다른 경로로 설치한 애플리케이션의 목록을 제공하여 사용자가 특이사항을 확인할 수 있도록 한다.

스크린샷이(가) 표시된 사진

자동 생성된 설명

그림 4) 앱 사용 분석 UI 설계

**3.2.4 다운로드 파일 분석**

내장메모리 내의 다운로드 파일들을 분석한다. 이미지, 동영상, 오디오, 문서, 설치파일 등 메모리 내의 다운로드 파일들의 종류와 비율을 분석하여 그래프로 제공한다. 시간대 별 다운로드 패턴을 분석하여 사용자의 다운로드 특성을 파악한다.

출처가 존재하는 다운로드 파일들의 출처를 표시하고 비슷한 출처에 따라 분류한다. 특정 기간 동안 다운로드 된 파일을 찾을 수 있도록 검색기능을 제공하여 시간에 따라 검색이 용이하도록 한다.

스크린샷이(가) 표시된 사진

자동 생성된 설명

그림 5) 다운로드 파일 분석 UI 설계

**3.2.5 사진 분류**

사진 분류는 사진의 메타데이터를 이용한 분류와 사진 자체의 데이터를 이용한 분류로 나뉜다.

메타데이터를 이용한 분류 중 첫번째는 사진이 찍힌 시간과 저장된 날짜 데이터를 이용해 분류하고 선택한 날짜 또는 기간에 해당하는 사진에 대한 검색 기능을 제공한다. 두번째는 사진의 위치 데이터를 이용해 사진의 위치를 지도에 마크하고 지도의 확대 정도에 따라 중심으로부터 가까운 위치의 사진을 그룹화한다.

사진데이터를 이용한 분류는 머신러닝을 이용해 사진의 종류를 분류한다. 자연 인물, 동물, 음식 등으로 기본 레이블을 설정하고 분류해 그룹화한다

텍스트이(가) 표시된 사진

자동 생성된 설명사진, 다른이(가) 표시된 사진

자동 생성된 설명

그림 6,7) 사진 분류 UI 설계 main과 detail(location)

**3.2.6 사용자 하루 타임라인**

추출한 모든 시간데이터를 기반으로 사용자의 하루를 정리하여 하나의 타임라인으로 제시한다. 사진 촬영 시간, 앱 사용 시간, 통화시작, 종료 및 지속시간, 문자 발신 및 수신 시간 등을 이용한다.

기본으로 어제의 타임라인이 제공되고 날짜를 지정해 그 날짜의 타임라인을 생성할 수 있다. 타임라인에 사용자의 코멘트를 더할 수 있고 이미지 파일로 export할 수 있다.

스크린샷이(가) 표시된 사진

자동 생성된 설명

그림 8) 사용자 하루 타임라인 UI 설계

**4. 결론 및 향후연구**

본 논문에서는 논리적 추출의 안드로이드 api(content provider)를 이용해 스마트폰에 존재하는 데이터를 추출 및 분석하는 도구를 만든다. 안드로이드 버전 업데이트와 새로운 기기 출시에 따른 보안성 향상으로 대부분의 모바일 포렌식 도구가 사용하는 Rooting kernel이나 물리적 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 포렌식 도구는 안드로이드 기반 스마트폰에서 추출할 수 있는 데이터와 그 목록을 제공하고, 6가지 주제로 세부 분석한 결과를 시각화 하여 보여준다. 데이터의 나열뿐만 아니라 시각화 된 정보도 제공하기 때문에 사용자가 데이터 해석을 할 때 시간적인 측면에서 도움을 줄 수 있을 것으로 예상된다.

향후 연구로는 Content provider로 얻기 힘든 데이터에 대한 추출 및 분석 기능 개발이 있다.

[참고문헌]

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