|  |
| --- |
| **안드로이드 WIFI 디지털 포렌식**  **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. 본 논문에서는 디지털 포렌식을 위한 안드로이드 스마트폰에 대한 데이터분석 및 수집 방법을 제안한다. 제안하는 방법은 안드로이드 스마트폰 포렌식의 기초 데이터를 만들고, 결론적으로 안드로이드 운영체제에서 포렌식을 수행할 수 있는 기반을 만들고자 한다. |

**1. 서론**

**1.1. 연구배경**

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. 디지털 포렌식은 범죄 재현이나 파괴적이고 비인가된 행동들에 대한 예측을 손쉽게 하기 위해 디지털 증거물에 대한 보존/수집/확인/식별/분석/해석/기록/현출을 과학적인 원리에 의해 도출하고 검증된 방법을 통해 수행하는 것을 의미한다. 포렌식 기술은 앞으로 점점 스마트폰을 이용한 범죄에 필수적인 기술로 자리 잡을 예정이며, 더 많은 연구가 요구되고 있다.

각종 디지털 기기가 보급되면서 디지털 기기에 저장되어 있는 데이터가 범죄 사실을 입증하는 증거로 사용되는 사례가 증가하고 있다.

안드로이드에서 데이터를 수집하기 위해서는 ADB를 활용하는 방법이 가장 편리하였고, 루팅을 하지 않고 얻을 수 있는 데이터에 초점을 맞추었다.

이중 와이파이를 통해 사용자의 동선을 추적할 수 있다는 판단이 들어 와이파이에 대한 내용들을 본 연구의 목표로 잡았다.

**1.2. 연구목표**

디지털 포렌식을 위해서는 무결성과 진정성에 대한 원칙을 지켜야 한다. 무결성은 디지털 데이터의 특성상 위변조와 훼손이 용이하기 때문에 세심하게 다뤄야 하며, 수집 이후 변경되지 않았음을 입증할 수 있어야 한다는 점이다. 진정성은 법정에 제출되는 모든 증거는 범죄 현장에 존재한 것이어야 한다는 것이다. 이번 연구는 기존 연구에서의 루팅 후 데이터 수집 방법과 다르게 루팅을 하지않고 데이터를 유지한 채 데이터를 추출할 수 있는 것을 기준으로 삼고 있다.

또한 와이파이는 현재 우리나라에 굉장히 많이 보급되어 있기 때문에 와이파이의 기록을 추적한다면 개통이 되어있지 않은 안드로이드 기기의 동선 또한 추적할 수 있을 것이라고 판단했다.

**2. 관련연구**

**2.1 덤프**

갤럭시 핸드폰의 파일시스템을 통째로 파일로 추출하는 방법이다. 파일시스템 뿐만 아니라 다른 여러 정보 또한 같이 추출한다.

**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.

**2.3 시스템 덤프**

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



그림 1 안드로이드 모바일기기의 시스템 데이터 제목 및 파일 경로

[그림 1]은 기존 연구 중 안드로이드 모바일 기기의 시스템 데이터 파일 경로를 나타내고 있다[2]. 안드로이드 버전이 올라감에 따라 내부 데이터 접근이 더욱 어려워졌으며, ADB 툴을 이용하여 데이터를 추출하는 데 한계가 있다.

본 장에서는 2가지 문제를 제시한다. 첫째는 루팅 없이 갤럭시 스마트폰에 접근할 수 있는 데이터는 한정되어 있다는 점이다. 두 번째 문제는 ADB를 통해 수집할 수 있는 데이터를 수집해본 결과, 실제 데이터에 접근할 수 없도록 암호화가 되어 있는 파일들이 존재한다는 점이다.

첫 번째 문제를 해결하기 위해 여러 가지 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 루트권한을 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.

두 번째로 물리적으로 메모리를 추출하여 파일시스템에 접근하는 방법은 추가 작업이 필요 없이 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 하이재킹을 할 경우, 물리적, 논리적 손상 없이 데이터를 추출할 수 있다는 장점이 있다. 다만 실제로 하이재킹을 위한 연구를 추가 진행해야 한다는 단점이 있다.

아래 [표 1]은 스마트폰 데이터 접근 방안별 장단점을 정리한 표이다.

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 |

두 번째 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..

**2.4 기존 연구의 문제점 및 해결 방안**

**2.4.1. 연구의 문제점**

안드로이드 운영체제에 접근 가능하지 않은 데이터를 추출하기 위한 연구가 필요하며 삭제된 데이터에 대한 복구 기술에 대한 연구도 필요하다고 생각한다.

루팅 시 기존 데이터가 삭제되는 문제점이 있어 데이터를 건드리지 않은 채 추출해야 한다는 점을 시사한다.

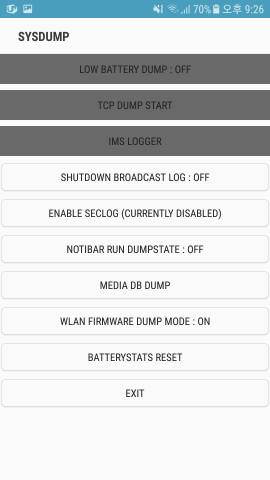
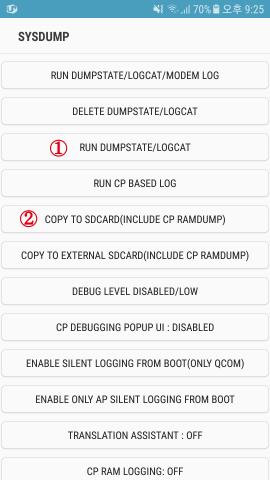
**2.4.2. 해결 방안**

**2.4.2.1  ADB(Android Debug Bridge, 이하 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.

ﾠ

**2.4.2.2 Sysdump**



Sysdump로써 "dumpState\_버전명\_생성일자.log" 파일이 Bugreport의 형식과 유사한 산출물이고 주요 분석대상이다.

**3. 프로젝트 내용**

**3.1. 시나리오**

**텍스트이(가) 표시된 사진

자동 생성된 설명**

포렌식 구성에 맞는 순서에 따라 오른쪽과 같이 프로그램을 제작하였다.

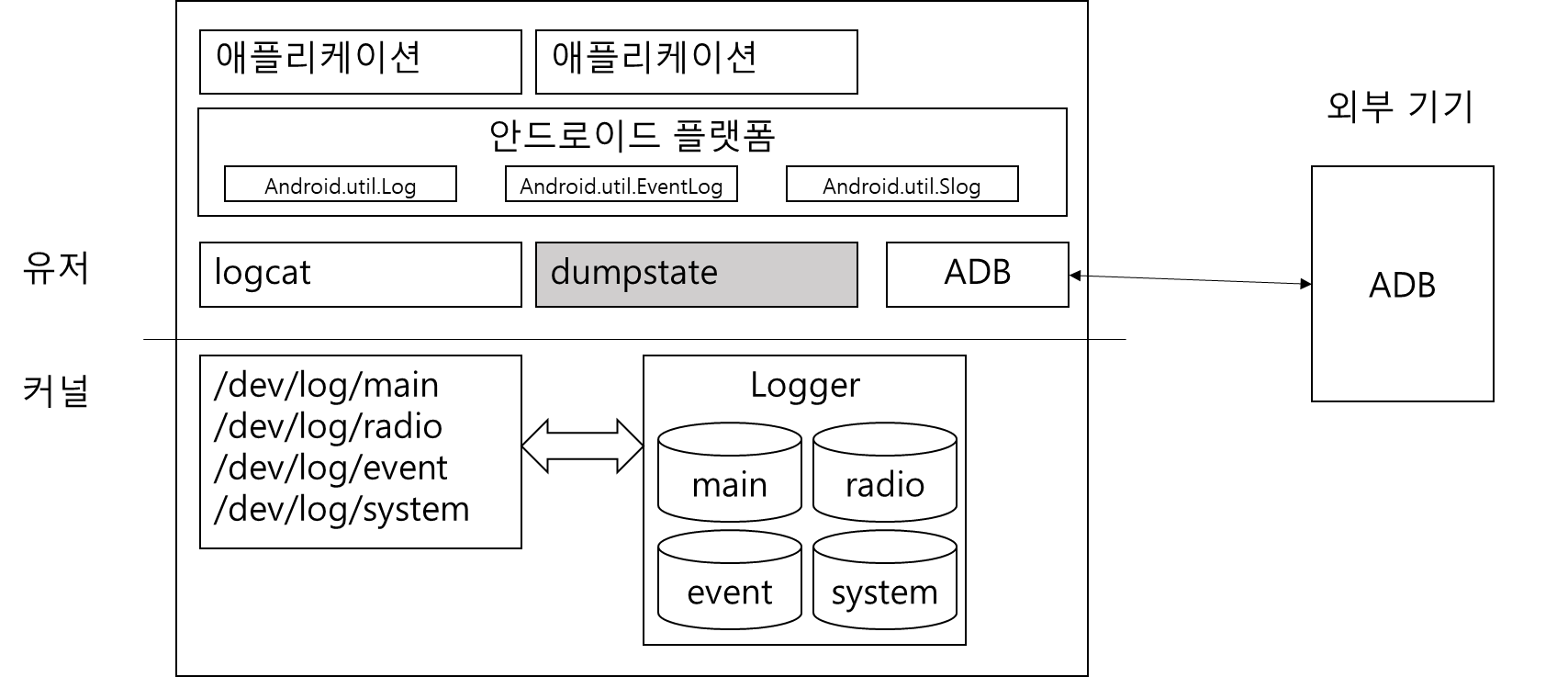
**3.2. 구현**

소스코드 경로 및 폴더 구성은 아래의 깃허브 링크를 통해 확인할 수 있다.

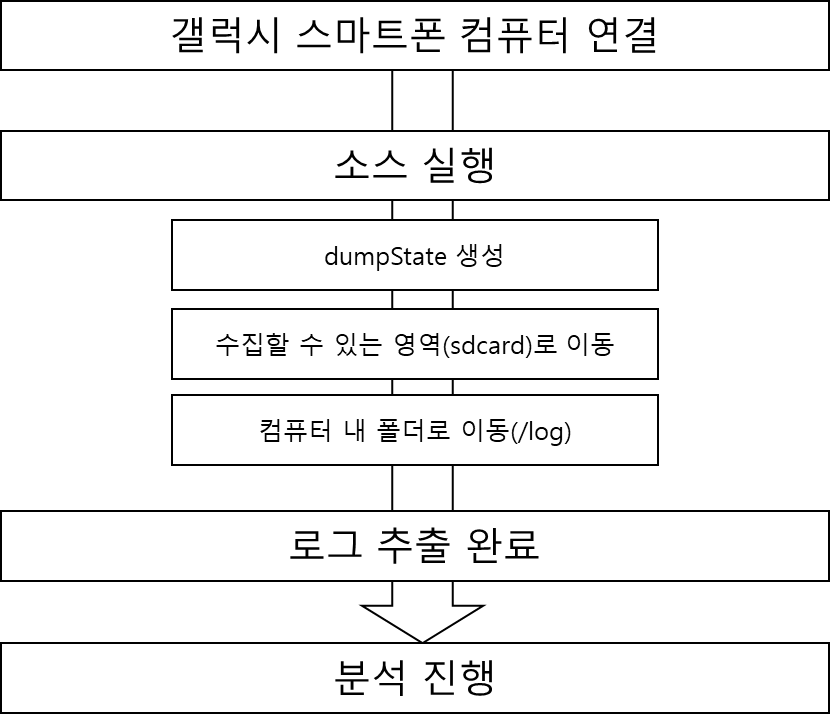
https://github.com/galaxy-forensic/Wififorensic

**4. 프로젝트 결과**

**4.1. 연구 결과**

****

안드로이드는 위와 같은 로그 시스템을 가지고 있다. 위의 도식표를 확인하였을 때 커널은 루팅을 해야 접근할 수 있는 곳이며 유저가 접근할 수 있는 곳 중 dumpstate에 대하여 ADB를 활용하여 로그를 자동으로 추출하는 프로그램을 개발한다.

****

위와 같은 순서로 로그 자동 추출 프로그램을 완성한다.

**3.2 WIFI 기록 분석**

**텍스트이(가) 표시된 사진

자동 생성된 설명**

우선 Wifi기록이 담기는 파일들을 LOG파일에서 확인하였다.

**텍스트이(가) 표시된 사진

자동 생성된 설명**

이중 WifiConfigManager라는 로그기록에서 해당 기기의 와이파이 접속 기록을 확인할 수 있다.

**텍스트이(가) 표시된 사진

자동 생성된 설명**

또한 와이파이 접속 시도를 분석한다. 근처 와이파이의 SSID 및 해당 MAC 주소를 확인할 수 있다.

텍스트이(가) 표시된 사진

자동 생성된 설명

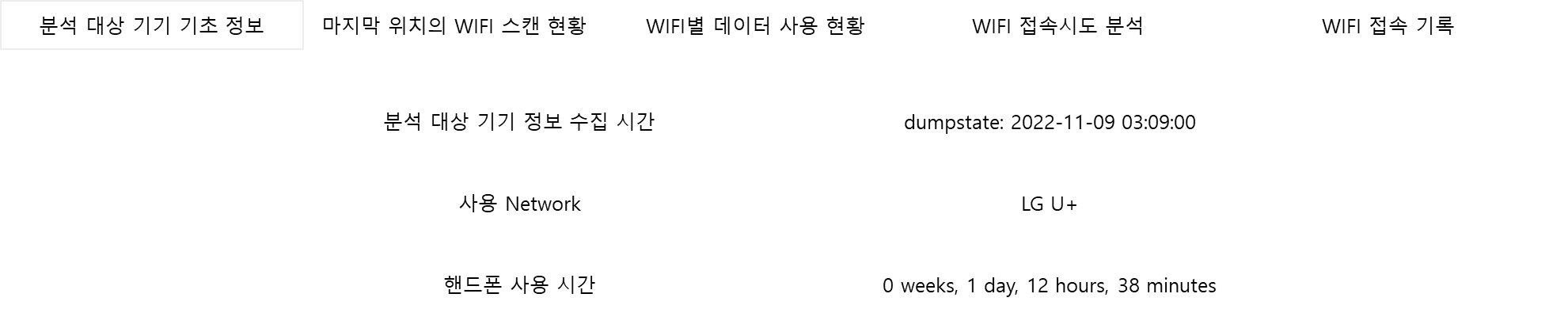
마지막으로 스캔한 와이파이 및 해당 SSID, 감도 등을 확인할 수 있다.

텍스트이(가) 표시된 사진

자동 생성된 설명

와이파이 접속 SSID 별 데이터 기록을 확인할 수 있다.

**3.3 시각화 진행**

****

분석 대상 기기에 대한 기초 정보를 확인할 수 있는 화면이다.

텍스트이(가) 표시된 사진

자동 생성된 설명

기기를 습득하였을 때 마지막 WIFI 스캔현황을 확인할 수 있다.

텍스트이(가) 표시된 사진

자동 생성된 설명

접속한 WIFI 별 총 접속시간 및 평균 데이터 사용량, 실 데이터 사용 기록을 확인할 수 있다.

텍스트이(가) 표시된 사진

자동 생성된 설명

시간대별 WIFI 접속시도를 분석할 수 있는 화면이며 위에서부터 신호가 높은 순서대로 정렬된다.

테이블이(가) 표시된 사진

자동 생성된 설명

실제 WIFI에 언제 연결되고 연결이 끊어졌는지 볼 수 있는 화면이다.

**4. 결론**

**4.1. 기대효과**

안드로이드 기기를 활용하면 WIFI를 키고 돌아다니는 것이 일반적이다. 3초마다 한번씩 와이파이를 스캔하는 기록을 발견하였으며 이를 타임스탬프와 함께 확인하여 동선을 추적할 수 있을 것이라 판단한다. 기존 포렌식의 경우 핸드폰의 네트워크 접속 기록을 확인하여 대략적인 위치 추적이 가능했지만, 이는 개통되지 않은 안드로이드 기기의 경우 WIFI를 통해 동선을 추적할 수 있을 것이라고 판단한다.

**4.2. 추후 연구 방향**

로그를 더 분석하여 WIFI 이외에도 다른 정보들이 있는지 확인해봐야 한다. 또한 이러한 sysdump는 안드로이드 개발 시 로그를 보기위해 만드는 것인데, 이는 추후 보안에 이슈가 생길 수 있으므로 삭제하는 방향으로 안드로이드 측에서 추가 개발이 진행되어야 할 것으로 보인다.