**갤럭시 디지털 포렌식**

**요약**

포렌식은 전자적 증거물 등을 사법기관에 제출하기 위해 데이터를 수집, 분석, 보고서를 작성하는 일련의 작업을 말한다. 과거에 얻을 수 없었던 증거나 단서들을 제공해 준다는 점에서 획기적인 방법이다. 그래서 포렌식을 통해 휴대폰에 어떤 데이터가 있는지 분석하려고 한다. 하지만 시스템 데이터를 얻기 위해서는 루팅이 필요하기 때문에 루팅 전후 데이터 비교를 시각화해서 보여줄 예정이다.

1. **서론**
   1. **연구 배경**

스마트폰이 등장하고 나서 스마트폰은 개인 정보를 가장 많이 담고 있는 도구가 되었고 이때문에 범죄의 표적이 되기도 한다. 또한 범죄에도 직접 쓰이기도 하는데 이런 범죄 활동을 법정에서 증명하는데 스마트폰은 결정적인 역할을 하기도 한다. 그 역할을 해줄 수 있게 해주는 기술을 디지털 포렌식이라고 한다. 디지털 포렌식은 디지털 증거물을 분석하여 수사에 활용하고, 디지털 증거물의 증거 능력을 향상시키기 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, 분석을 하는 포렌식 도구를 개발하려고 한다.

본 연구에서는 데이터를 수집, 분석을 하는 기존의 포렌식 방식을 안드로이드 폰인 ‘갤럭시’ 시리즈에 적용해보는 연구를 진행할 예정이다.

* 1. **연구 목표**

안드로이드 운영체제를 사용하는 ‘갤럭시’ 시리즈 폰의 데이터를 수집, 분석하고 분석한 데이터를 통해 어떠한 데이터가 시스템 데이터에 들어있는지를 시각화 하는 작업을 진행할 예정이다. 이를 위해 안드로이드 시스템 배경, ADB 아키텍처 및 디지털 포렌식의 기본 원칙을 포함하여 시스템 연구를 진행할 것이며, 시스템 데이터를 얻기 위해 갤럭시 폰에 루팅을 진행한 후 데이터를 추출, 분석할 계획이다. 이 데이터를 시각화 하는 작업은 react를 통해 웹으로 보여줄 예정이며, 모든 사용자 데이터를 보여주는 것이 아닌 특정 사용자 데이터를 선정 후 웹으로 보여줄 예정이다.

1. **관련연구**
   1. **덤프**

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

* 1. **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.

* 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 업/다운로드, 시스템 log 출력, shell 접속 등이 가능하다. 따라서 접근이 제한되어 있는 애플리케이션의 데이터에 대해 복원, 추출이 가능하게 해준다.

* 1. **React**

리액트는 자바스크립트 라이브러리의 하나로서 사용자 인터페이스를 만들기 위해 사용된다. 페이스북과 개별 개발자 및 기업들 공동체에 의해 유지보수된다. 리액트는 싱글 페이지 애플리케이션이나 모바일 애플리케이션 개발에 사용될 수 있다

* 1. **기존 연구의 문제점 및 해결 방안**
     1. **연구의 문제점**

루팅한 데이터를 추출 후 분석을 했는데 루팅을 하고 나니 사용자의 모든 데이터가 초기화가 되어서 제한된 데이터를 분석을 해야 하는 환경이었다. 그래서 사용자 데이터 분석을 원활하게 하지 못했으며 어떤 데이터가 루팅 후에 추출되었는지 알기 쉽지 않았다.

* + 1. **해결 방안**

루팅을 한 후 사용자 데이터에 접근이 가능해졌고, 이를 통해 어떤 사용자 데이터가 갤럭시 속에 있었는데 분석이 가능해졌다. 이를 통해 사용자 데이터를 분석 후 어떤 데이터가 갤럭시에 있는지 루팅 전후로 나누어서 루팅을 하면 얻을 수 있는 데이터에 대해 시각화를 진행할 예정이다.

**3. 프로젝트 내용**

**3.1. 시나리오**

**3.1.1. 파일시스템 덤프**

실험 대상인 갤럭시 핸드폰에 대해 파일시스템을 통째로 Dump 하여 파일로 추출한다. 또한 현재 실행 중인 메모리, 앱 설치 목록 등 함께 추출할 수 있는 정보 또한 같이 추출한다. 이 Dump를 진행한 후 사용자 데이터를 얻기 위해 루팅을 진행하고 똑같은 방식으로 Dump를 진행해서 루팅 하기 전에 데이터와 루팅 후의 데이터를 각각 추출한다.

**3.1.2. 파일시스템 분석**

루팅한 데이터에서 나온 로그들과 데이터를 분석하여 어떤 정보가 로그와 데이터에 들어있는지 분석을 하고 이 데이터가 루팅을 해야만 얻을 수 있는 데이터인지 파악을 할 것이다. 아래의 분석 결과는 루팅 후 Dump를 통해 얻은 로그들과 데이터베이스 파일을 분석하여 주요 파일을 표로 정리한 것이다.

주요 로그 파일 분석 결과

|  |  |
| --- | --- |
| 파일명 | 저장 데이터 |
| power\_off\_reset\_reason.txt | 전원 관련 로그 저장 |
| qtables.json | 네트워크 접근 기록 저장 |
| Iwc\_dump.txt | WIFI 접근 기록 저장 |
| subBuffer.log | 블루투스 접근 기록 저장 |
| CallContent.log | 전화 기록 저장 |
| Recovery\_history.log | 복구 기록 저장 |
| Settingsprovider.txt | 핸드폰의 세팅 변경 기록 저장 |
| Shutdown\_profile.n.txt (n은 1이상 숫자) | 기기의 종료 기록 저장 |
| Packages.xml | 어플리케이션의 목록 및 각각의 권한 저장 |
| n/Settings\_config.xml (n은 0이상 숫자) | 사용자별 기기 세팅 정보 저장 |

주요 데이터베이스 파일 분석 결과

|  |  |
| --- | --- |
| 파일명 | 저장 데이터 |
| Audioservice\_sec.db | 어플리케이션의 오디오 권한 저장 |
| ClipboardimageTable.db | 클립보드에 있는 스크린샷 파일 목록 저장 |
| Displaysolution\_setting.db | 화면 권한 설정 저장 |
| Enterprise.db | 기기의 전반적인 설정 저장 |
| Gamemanager.db | 게임 매니저에 관한 앱과 로그 저장 |
| Locksettings.db | 화면 잠금에 대한 정보 저장 |
| Notification.db | 알림들의 로그 저장 |
| Pda.db | 단말기 정보 저장 |
| Pkgpredictions.db | 패키지 정보 저장 |
| Psitracker.db | Psi 측정정보 저장 |
| Recoverablekeystore.db | 클라우드 정보 저장 |
| wifihistory.db | 와이파이 사용 기록 저장 |

**3.1.3. 추가 분석 대상 탐색 및 시각화**

루팅을 하기전에 데이터와 루팅을 한 후의 데이터에 대해 비교 분석을 진행한 후에 사용자의 어떤 데이터가 루팅을 해야지만 얻을 수 있는지에 대해 파악을 하고 이 데이터에 대해 시각화를 진행할 예정이다.

**3.2. 요구사항**

**3.2.1. 파일시스템 덤프에 대한 요구사항**

파일시스템 및 메모리 전체에 대한 덤프가 요구된다. 사용되지 않는 파일시스템 부분이라 할지라도 추후 추가연구를 위해 필요하기 때문에 파일시스템 전체에 대한 메모리 덤프가 요구된다.

추가적으로 이 모든 과정이 추후 자동으로 이루어져야 하는 점을 고려해, 모듈화 시켜 개발할 필요가 있다.

**4. 향후 일정 및 역할 분담**

10월까지 데이터를 비교 분석을 진행하고, 이 결과를 바탕으로 시각화 할 데이터를 선정할 것이다. 그리고 이 선정한 데이터를 React를 통해 시각화를 진행하여 웹으로 보여줄 예정이다.

**5. 결론 및 기대효과**

본 연구는 기존에 진행되었던 포렌식 도구 개발 연구와 다르게 핸드폰 제조회사에서 제공하는 정보 외의 데이터를 취급하기 위해 파일시스템에 직접 접근한다. 이로 인해 훨씬 더 원시적인 데이터에 접근할 수 있게 될 것이다. 스마트폰을 분리하지 않은 채로 사용자의 데이터를 모두 얻어낸다면, 추후 포렌식 관련 연구에서 사용자가 숨기려고 한 데이터 또한 추출이 가능할 것이다. 또한 이 추출된 데이터를 비교 분석한 후 시각화를 통해 접근성 또한 높여줄 계획이다.

**6. 참고문헌**

[1] https://www.xda-developers.com/how-to-install-magisk/