갤럭시 디지털 포렌식 도구

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. 따라서 갤럭시 폰을 포렌식 하기 위해 파일 시스템의 분석, 삭제 파일과 암호화 파일의 구조를 파악하는 연구를 진행할 예정이다.

1 서론

1.1 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.

1.2 연구 목표

안드로이드 운영체제를 사용하는 '갤럭시' 시리즈 폰의 데이터를 수집, 분석하며, 삭제된 데이터를 복구 시키는 연구까지 진행할 예정이다. 이를 위해 안드로이드 시스템 배경, ADB 아키텍처 및 디지털 포렌식의 기본 원칙을 포함하여 시스템 연구를 진행할 것이며, 최종적으로는 갤럭시 핸드폰에 대해 파일시스템을 통째로 Dump 하여 파일로 추출 후 포렌식을 진행한다.

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 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.

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.

2.4.2 해결 방안

파일시스템 자체에 접근을 하게 된다면 어플리케이션 혹은 사용자가 직접 접근을 막았던 파일에도 접근을 할 수 있게 된다.

또한 추가적으로 앱 별 파일 저장방식 및 암호화 등에 대한 연구가 추가적으로 이루어진다면 갤럭시 시리즈의 스마트폰에 대한 포렌식은 완벽하게 이루어질 수 있을 것이라고 생각한다.

3. 프로젝트 내용

3.1. 시나리오

3.1.1. 파일시스템 덤프

실험 대상인 갤럭시 핸드폰에 대해 파일시스템을 통째로 Dump 하여 파일로 추출한다. 또한 현재 실행중인 메모리, 앱 설치목록 등 함께 추출할 수 있는 정보 또한 같이 추출한다.

3.1.2. 파일시스템 분석

기존 알려진 표준 안드로이드 파티션을 기준으로 분석을 진행한다. 우리의 주 연구 대상은 userdata 가 될 것이다. 다만 파티션은 삼성이나 LG, HTC 와 같이 각 벤더에 따라 다른 파티션이 있을 수 있으므로 추가 분석을 진행한다.

영역 이름명	포맷	설명
Boot	Bootimg	커널+initramfs(램디스크), 부팅을 위한 커널 및 램디스크가 있는 공간
Cache	Ext4	안드로이드 /cache, 업데이트 및 복구에 사용
Recovery	Bootimg	부트-복구 : 시스템 복구를 위한 커널 + 다른 initramfs
System	Ext4	안드로이드 /system, OS 바이너리와 프레임워크
userdata	Ext4 / F2Fs	안드로이드 /data, 사용자 데이터와 설정

3.1.3. 추가 분석 대상 탐색 및 자동 분석

삭제된 파일 복구, 앱 별 파일 저장방식 연구 등을 연구하여 추후 사용자가 숨기려고 했던 파일 혹은 앱 내부 구조를 파악하여 자동으로 포렌식을 진행할 수 있는 프로그램을 개발한다.

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

4 월 중으로 파일시스템 덤프 및 분석 결과를 도출한다. 또한 파일시스템 분석결과에 따라 추후 6 월까지 진행하는 추가 분석 계획을 도출하도록 한다.

5. 결론 및 기대효과

본 연구는 기존 캡스톤디자인 1 에서 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.

6. 참고문헌

[1] https://kofboy2000.tistory.com/22

[2] https://codechacha.com/ko/android-adb-dump-heap/