모바일 OS 아티팩트 분석 및 검증 연구

모바일 아티팩트
모바일 기기에서 다양한 서비스를 제공하기 위해 수집하는 사용 시간, 사용 위치, 대화 내용 등의 데이터 중 사용자의 행위를 유추할 수 있는 데이터

- 모바일 OS는 모바일 기기가 동작하기 위해 필수적으로 사용되는 특징이 존재함.
  - -> 모바일 기기가 사용된 사건에서 반드시 모바일 OS 아티팩트가 검출되기 때문에 모바일 포렌식 수사에 범용적으로 활용 가능함. 추가로 모바일 포렌식 수사를 위한 선별 압수에 활용될 수 있음.

기존 연구들의 한계

- 기존 모바일 기기에서 아티팩트 분석에 관한 연구들이 수행됐으나 대상 기기의 제조사, 시리즈, 버전, OS 버전 등이 각각 상이하므로 다른 모바일 기기에 대한 적용 가능 여부를 파악하기 힘듦.
- 모바일 아티팩트에 관한 대부분의 기존 연구들은 사용량이 많은 서드 파티 애플리케이션을 대상으로 진행되어 해당 애플리케이션을 사용하지 않은 사건에는 적용하기 어려움.
- 기존 연구의 연구 대상 모바일 기기는 기종과 모바일 OS 버전이 한정되어 있으며, 모바일 기기의 아티팩트는 모바일 OS의 버전, 대상 모바일 기기의 제조사 및 기종에 따라 변화할 수 있음.
  - -> 기존 연구 결과에서 제시된 아티팩트를 획득하려 했을 때, 기존 연구와 동일한 기기 및 OS 버전에 대해서 아티팩트를 획득할 수 있는지 여부는 검증되지 않았음.
    - -> 아티팩트 수집 및 활용 여부 불투명
  - 한정된 범위의 연구는 지속적으로 변화하는 모바일 기기의 특성에 대응하지 못한다는 단점을 지님.

결론
본 논문은 기존 연구 결과로 제시된 모바일 아티팩트에 변화 가능성을 제시하며 기존 연구의 확장 필요성을 제시함. 또한, 기존 연구들은 서드 파티 애플리케이션 아티팩트 위주로 진행됨.(카톡, 페북, 디코 등) 하지만 용의자가 해당 서드 파티 애플리케이션을 사용하지 않았을 경우에는 수사에 도움이 되지 않음. 이러한 이유를 들어 모바일 OS 아티팩트에 대한 연구 필요성 제시함.

Methodology
본 논문은 위와 같은 기존 연구의 한계를 보완하기 위해 연구 대상을 서드 파티 애플리케이션이 아닌 모바일 [1]OS 아티팩트로 설정.

<사용한 안드로이드 기기 및 OS>

1. Samsumg Galaxy S7 edge + android 6, 7

2. Samsumg Galaxy S8 + android 7, 8
3. Samsumg Galaxy S9+ + android 9, 10
4. Samsumg Galaxy S10 5G + android 10

<분석 도구>

1. MD-NEXT, MD-RED << 유료;;
   이미징 및 이미징 파일 분석에 사용
2. Cellebtie UFED << 유료;;
   스마트폰 OS의 물리 및 논리 데이터 획득을 지원, 이미징 파일과 파일 시스템 내의 파일들에 대해 해시값을 계산하여 제공 -> 무결성 입증
3. Android Debug Bridge(ADB)
   애플리케이션 설치, 디버깅, 파일 송수신 등 안드로이드 기기 조작 가능. 본 연구에서는 adb shell 명령어를 통해 대상 기기에 접속하여 아티팩트를 확인하고, 데이터베이스 파일 등의 추가적인 뷰어가 필요한 경우 adb pull 명령어를 사용하여 파일 추출. << 루팅하고 쓰이는 걸로 알고있음
4. HxD
   바이너리 데이터를 자동으로 문자열로 변환하는 기능을 통해 바이너리 파일의 데이터를 해석하기 위해 사용 << 이렇게도 사용할 수 있는지는 몰랏음 ㅎㅎ
5. DB browser for SQLite
   SQLite 데이터베이스의 뷰어 프로그램으로, 애플리케이션이 저장한 데이터베이스를 분석하기 위해 사용.

<분석 과정>

- 분석대상 기기에 USIM을 넣어 실사용하여 데이터를 축적한 후, 대상 기기를 포렌식하여 각각의 데이터를추출하는 방식으로 진행.
- 안드로이드 기기의 경우 루팅한 후, 같은 방식으로 진행하여 루팅 기기 및 루팅되지 않은 기기의 차이점을 확인.
- 루팅 기기에 adb를 이용하여 접속한 후, 실제 디렉토리와 포렌식 도구의 파일 시스템 추출 결과를 비교
- +) 기본적으로 [2]물리적 데이터 추출을 이용하나, 물리적 데이터 추출이 불가능한 경우에는 [3]논리적 데이터 추출 방법을 이용하여 데이터 추출
- Python을 이용하여 안드로이드에서 분석 대상 기기에 존재하는 아티팩트를 추출하는 프로그램을 제작해 아티팩트를 추출한 후 분석을 진행

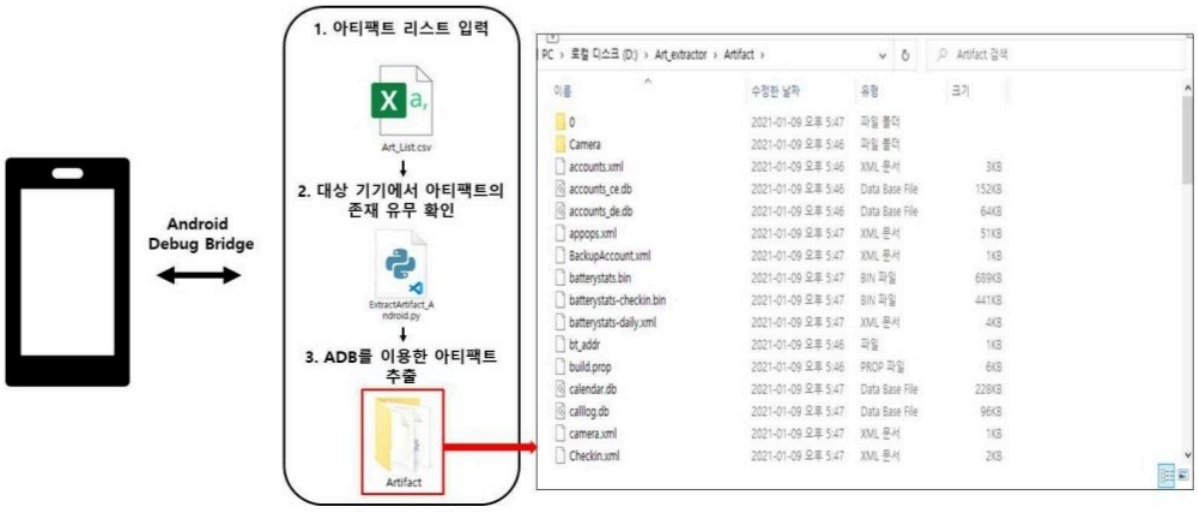


Fig. 4.3 안드로이드 아티팩트 추출 프로그램

ADB를 이용한 아티팩트 분석 과정

1. 루팅된 대상 기기와 분석용 데스크탑에 연결한 후, ADB를 이용하여 대상 기기에 접속해 대상 아티팩트의 경로로 이동한 후 아티팩트를 확인하는 방법
2. ADB의 [4]Bugreport를 이용한 방법

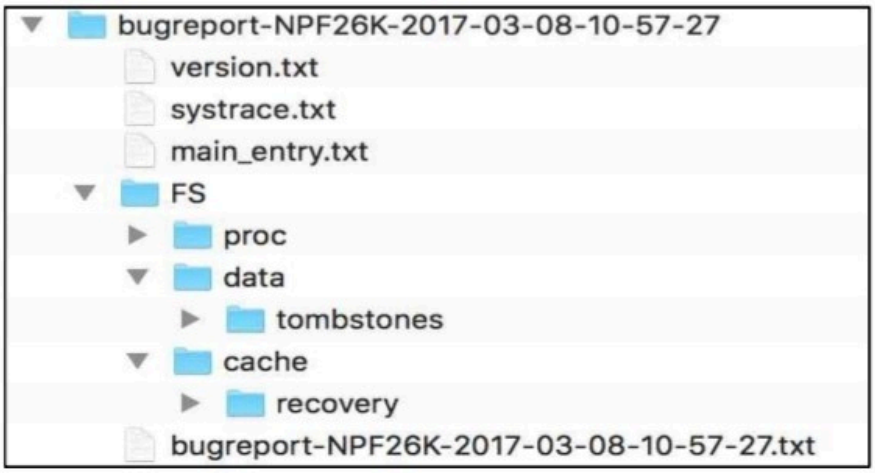


Fig. 4.4 안드로이드 Bugreport 파일 구조

- 기기를 데스크탑에 연결한 후, 아래와 같은 ADB 명령어를 통해 수집 가능.
  $ adb bugreport E:\Reports\MyBugReports
- 저장할 경로를 지정하지 않으면 ADB가 설치된 로컬 디렉터리에 zip 파일 생성됨.
  - bugreport-BUILD_ID-DATE.txt 파일에 dumpsys, dumpstate, logcat 등의 내용이 포함되어 있기 때문에 해당 파일을 집중적으로 분석.

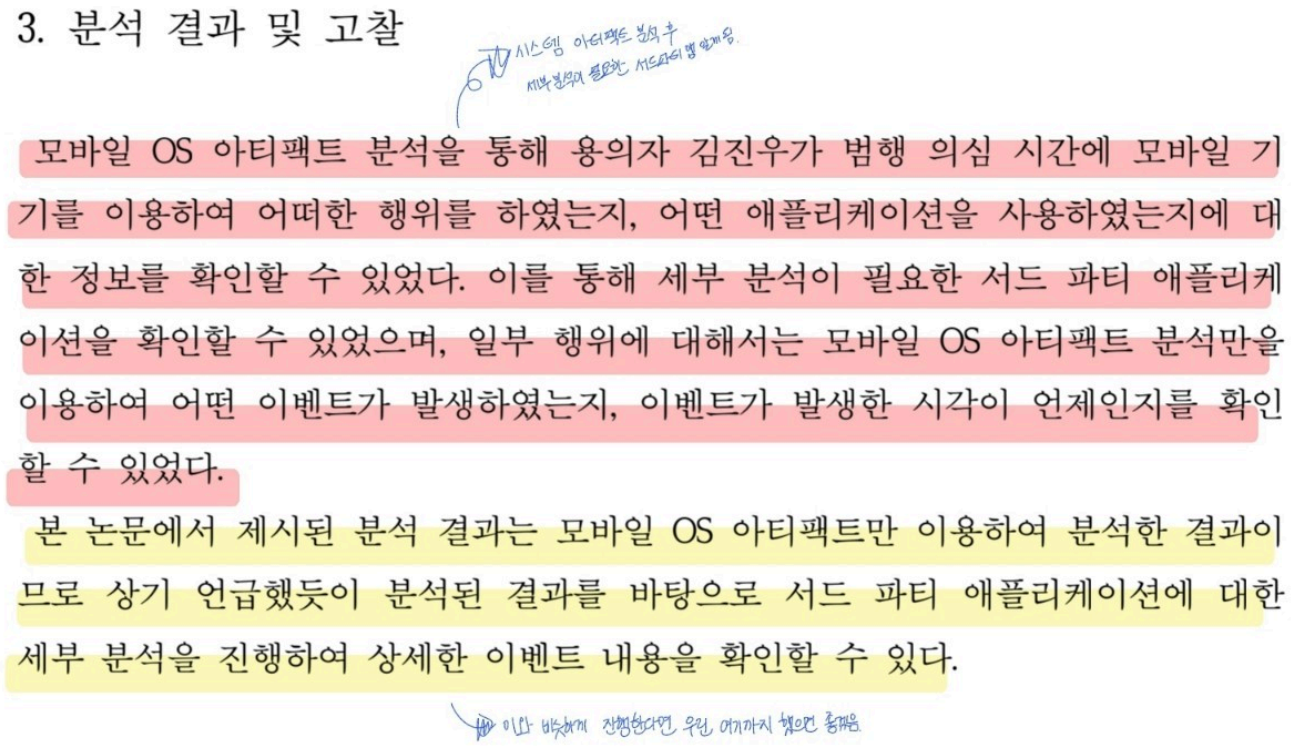
43개의 모바일 OS 아티팩트에 관한 기존 연구를 분석한 후, 확장 및 검증 실험을 통해 안드로이드 및 ios를 사용하는 주요 모바일 기기를 대상으로 모바일 OS 아티팩트에 대한 연구 결과를 분

류 및 정비하여 연구 결과를 제시함.

발표할 때 넣으면 좋을 것 같은 내용
(분석 과정 중 루팅에 대한 설명을 할 때) 해당 방법은 실제 포렌식 수사 과정에서는 루팅 시 데이터가 초기화되거나, 무결성이 훼손될 수 있으므로 사용하기 어렵다. 그러나 본 프로젝트에서는 [5]~를 위해 해당 방법을 이용하여 검증 실험을 진행하였다.

본 연구의 value
데이터 수집 단계에서는 선별 수집 과정에서 수집대상 데이터를 선정하기 위해 사용될 수 있으며, 분석 과정에서 사용자 행위 식별 관점으로 정리된 실험 결과를 이용하여 분석 효율성을 증대시킬 수 있음.

추가적으로...



3. 분석 결과 및 고찰

모바일 OS 아티팩트 분석을 통해 용의자 김진우가 범행 의심 시간에 모바일 기기를 이용하여 어떠한 행위를 하였는지, 어떤 애플리케이션을 사용하였는지에 대한 정보를 확인할 수 있었다. 이를 통해 세부 분석이 필요한 서드 파티 애플리케이션을 확인할 수 있었으며, 일부 행위에 대해서는 모바일 OS 아티팩트 분석만을 이용하여 어떤 이벤트가 발생하였는지, 이벤트가 발생한 시각이 언제인지를 확인할 수 있었다.

본 논문에서 제시된 분석 결과는 모바일 OS 아티팩트만 이용하여 분석한 결과이므로 상기 언급했듯이 분석된 결과를 바탕으로 서드 파티 애플리케이션에 대한 세부 분석을 진행하여 상세한 이벤트 내용을 확인할 수 있다.

---

1. 모바일 기기가 동작하기 위해 필수적으로 사용되기 때문에 연구 결과가 범용적으로 사용될 수 있음. ↩
2. 플래시 메모리 전체를 비트 단위로 복사하는 방법. 시간은 오래 걸리지만 비할당 영역의 데이터도 복사하기 때문에 스마트폰의 파일 시스템 및 펌웨어, 삭제된 파일, 슬랙 공간의 데이터도 추출 가능. ↩
3. USB를 이용하여 플래시메모리의 파일 시스템에서 저장된 파일 및 디렉토리를 추출하는 방법. 물리적 데이터 추출에 비해 시간은 적게 걸리지만, 삭제된 데이터나 슬랙 공간의 데이터는 추출할 수 없다는 단점이 있음. ↩
4. 안드로이드에서 버그가 발생했을 때, 이를 확인 및 분석하기 위해 운영체제에서 지원하는 기능.
   - dumpsys, dumpstate, logcat을 포함한 로그를 수집.

- 일반적으로 Bugreport의 분석은 휘발성이며, 최근에 기록된 소량의 기록만 확인할 수 있으나 시스템 로그는 사용자 의도와 관계없이 생성되는 파일로서 사용자가 조작하기 어렵다는 특징을 지님.
- USIM 교체 정보, 전원 관련 정보 등 기존의 분석 방법으로는 알 수 없는 정보를 포함하고 있어 분석이 필요함.

↩

5. 논문에서는 "포렌식 도구를 통한 분석과 비교 및 검증을 위해"라고 했음. ↩