Logcat 도구 개발 및 특허 현황

2024.09.27

모바일시스템공학과 조민혁

INDEX

01 Logcat 도구 개발

Logcat 도구 개발

❖Logcat의 문제점

✓ Logcat은 로그 데이터를 명령어를 통해 간편하게 볼 수 있다는 장점이 있지만, 전원 OFF 시 로그 데이터가 삭제된다는 특성이 있음

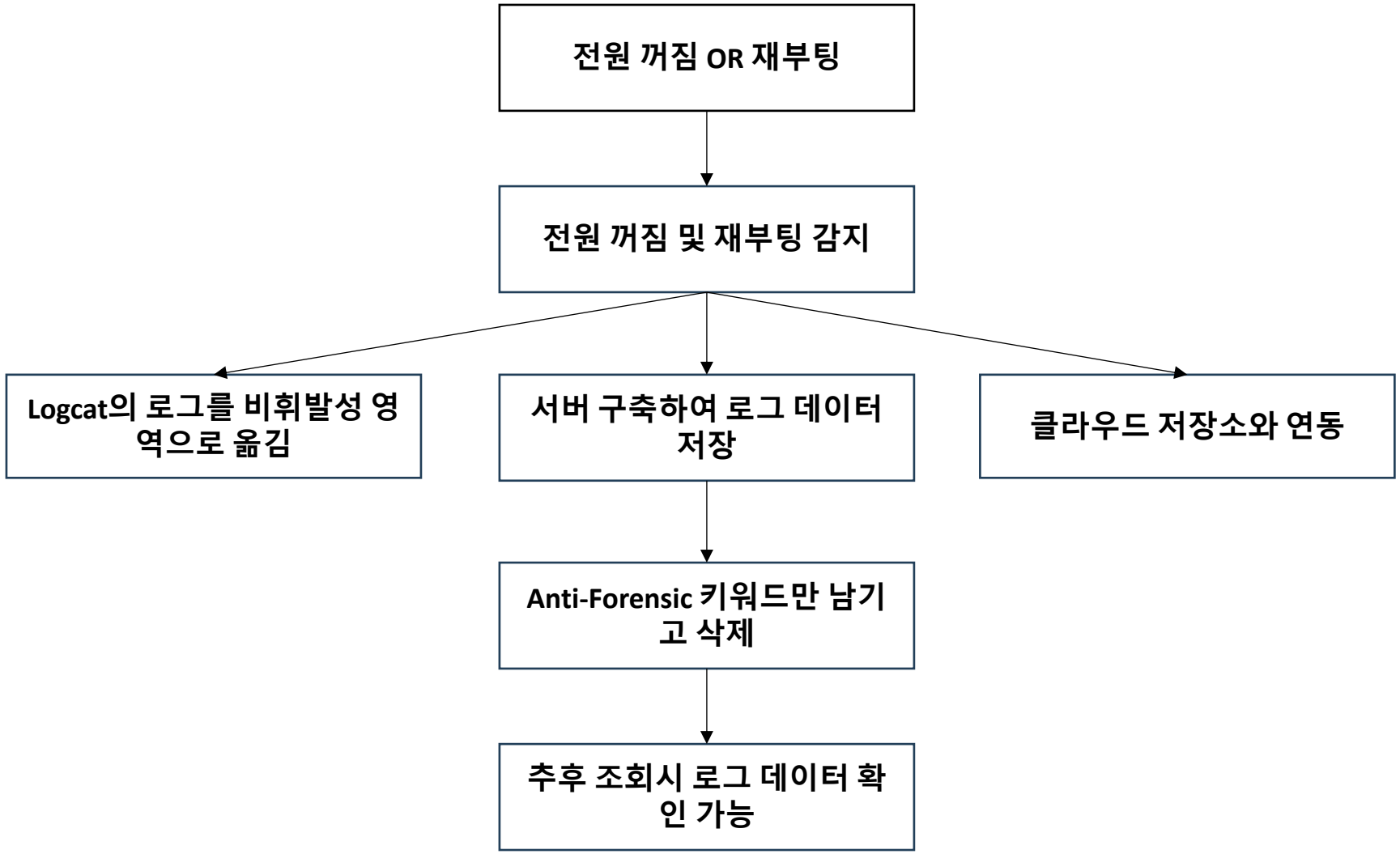
❖목적

✓ 휘발성 로그가 재부팅 또는 전원 꺼짐 감지 시 비휘발성 영역으로 옮겨져서 “안티-포렌식“ 키워드만 남기고, 삭제한다.

✓ 포렌식 수사 관점에서 개발

✓ 효율적인 포렌식 수사가 될 수 있도록 기여하는 측면에서 개발

Logcat 개발 순서도



개발 계획

❖도구 Ver.

✓ 프로그래밍 언어: C++

✓ 프레임워크: Native C++

❖어플 Ver.

✓ 프로그래밍 언어: Java

✓ 프레임워크: Android SDK, Android Jetpack

* 추후 공부하면서 수정될 수 있음

개발 현황 및 계획 (+논문 계획)

❖현재 자바 프로그래밍 문법 공부 (이번주(~09/27) 까지 공부 마칠 예정)

❖자바 문법 공부 후 프레임워크 공부와 더불어 시작

+ SCI 논문 투고를 위해 교수님께서 주신 아이디어를 바탕으로

  리빙랩 차량 실험 및 분석 예정

02 특허 현황

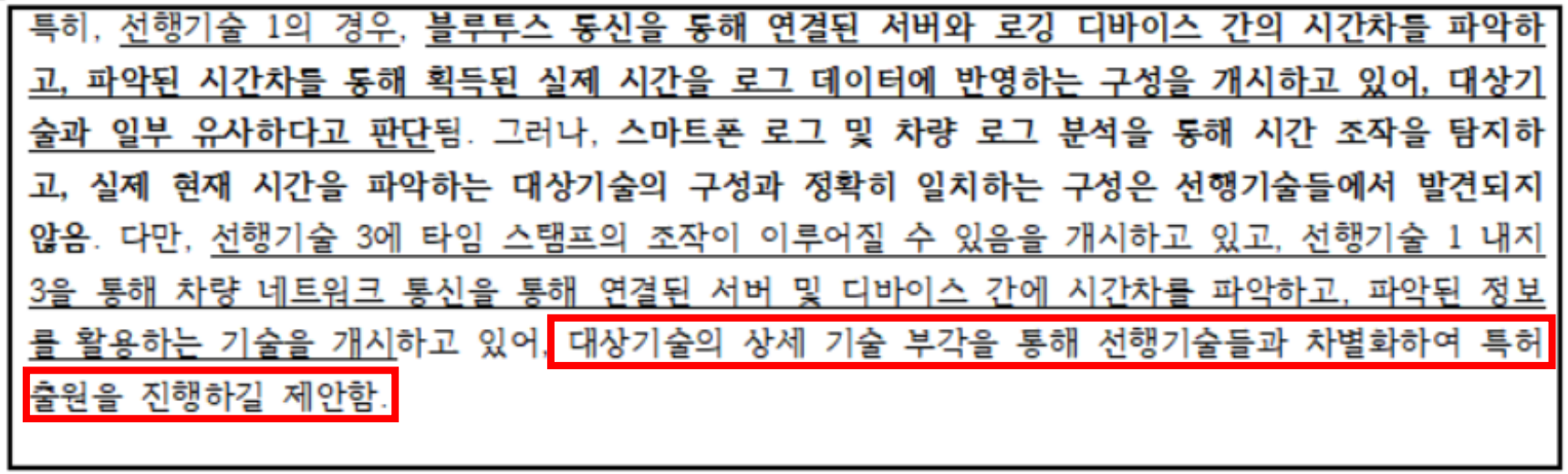
특허

❖ 특허 명세서

명 세 서
발명의 명칭
스마트폰과 연결된 차량 인포테인먼트 시스템에서의 시간 조작 탐지 기법
요약
본 발명은 블루투스를 통해 연결된 안드로이드 기기(특히 스마트폰과 자동차 간)에 대해, 범죄자가 타임스탬프를 조작했을 때 이를 탐지하는 효율적인 기법을 제공한다. 구체적으로, 본 발명은 안티 포렌식 행위 수사 과정에서 시간 조작을 탐지하고, 이를 통해 안티 포렌식 행위에 대한 수사 효율성을 극대화하는 프로세스를 제공한다.

특허 메일 피드백

❖변리사님의 피드백 1



특히, 선행기술 1의 경우, 블루투스 통신을 통해 연결된 서버와 로깅 디바이스 간의 시간차를 파악하고, 파악된 시간차를 통해 획득된 실제 시간을 로그 데이터에 반영하는 구성을 개시하고 있어, 대상기술과 일부 유사하다고 판단됨. 그러나, 스마트폰 로그 및 차량 로그 분석을 통해 시간 조작을 탐지하고, 실제 현재 시간을 파악하는 대상기술의 구성과 정확히 일치하는 구성은 선행기술들에서 발견되지 않음. 다만, 선행기술 3에 타임 스탬프의 조작이 이루어질 수 있음을 개시하고 있고, 선행기술 1 내지 3을 통해 차량 네트워크 통신을 통해 연결된 서버 및 디바이스 간에 시간차를 파악하고, 파악된 정보를 활용하는 기술을 개시하고 있어, 대상기술의 상세 기술 부각을 통해 선행기술들과 차별화하여 특허 출원을 진행하길 제안함.

궁금한 점1) 어떤 식으로 진행해야 할지 느낌이 없어서 방향성을 잡아 주시면 감사하겠습니다.

궁금한 점2) 특허명세서를 수정해야 하는건지 궁금합니다.

특허 메일 피드백

❖변리사님의 피드백 2

ⓐ 추출 대상 기기로부터 스마트폰/차량 로그(각각 블루투스 로그, 시스템 로그 포함) 수집하는 데이터 수집부

ⓑ 블루투스 로그 분석을 통해 타임스탬프 조작 가능성 의심 흔적을 발견하기 위한 분석부

ⓒ 시스템 로그 분석을 통해 시간 조작의 증거 탐지를 수행하는 증거 발견부

ⓓ 시스템 로그 분석을 통해 올바른 현재 시간 파악을 수행하는 시간 조정부

ⓔ 스마트폰의 경우, ADB 환경에서 'bugreport' 명령어를 사용하여 로그를 수집하고, 차량의 경우, 딜러 모드에서 로그를 수집하는 구성(추출 대상 기기에 따라 로그 추출 방법 상이)

ⓕ 스마트폰과 차량의 시스템 로그를 추가 분석하여 시간 조작과 관련된 로그 메시지를 확인하여 시간 조작 증거를 확인하되, 서로 다른 파일 확인을 통해 파악하는 구성

선행기술들은 대상기술의 주요 특징을 개시 또는 암시하지 않으므로, 대상기술의 주요 특징인 "추출 대상 기기로부터 스마트폰/차량 로그 수집하는 구성, 블루투스 로그 분석을 통해 타임스탬프 조작 가능성 의심 흔적을 발견하는 구성, 시스템 로그 분석을 통해 시간 조작의 증거 탐지를 수행하는 구성, 및 시스템 로그 분석을 통해 올바른 현재 시간 파악을 수행하는 특징(ⓐ + ⓑ + ⓒ + ⓓ)"으로 독립항을 구성하고 나머지 특징(ⓔ, ⓕ)은 종속항으로 구성하여 출원할 것을 제안드립니다.

감사합니다