【서지사항】

【서류명】 특허출원서

【참조번호】 0008

【출원구분】 특허출원

【출원인】

【명칭】 단국대학교 산학협력단

【특허고객번호】 2-2005-016634-4

【대리인】

【명칭】 특허법인린

【대리인번호】 9-2023-100001-3

【지정된변리사】 장영태, 박진철, 박진태

【포괄위임등록번호】 2024-018865-7

【발명의 국문명칭】 모바일 장치에서 발생한 이벤트 데이터를 수집하고 저장하는 장치 및 방법

【발명의 영문명칭】 Apparatus and method for collecting and storing event data from mobile device

【발명자】

【성명】 조성제

【성명의 영문표기】 CHO, Seong Je

【국적】 KR

【주민등록번호】 660209-1XXXXXX

【우편번호】 16832

【주소】 경기도 용인시 수지구 풍덕천로 161, 105동 302호 (풍덕천동, 수지마을동보아파트)

【거주국】 KR

【발명자】

【성명】 조민혁

【성명의 영문표기】 CHO, Min Hyuk

【국적】 KR

【주민등록번호】 000714-3XXXXXX

【우편번호】 12955

【주소】 경기도 하남시 대청로116번길 59, 408동 503호 (창우동, 꿈동산신안아파트)

【거주국】 KR

【발명자】

【성명】 이승민

【성명의 영문표기】 LEE, Seung Min

【국적】 KR

【주민등록번호】 010702-3XXXXXX

【우편번호】 15467

【주소】 경기도 안산시 단원구 안산천남로 245, 912동 1205호 (고잔동, 주공그린빌)

【거주국】 KR

【발명자】

【성명】 정성원

【성명의 영문표기】 JEONG, Seong Won

【국적】 KR

【주민등록번호】 011206-3XXXXXX

【우편번호】 07524

【주소】 서울특별시 강서구 허준로 23, 108동 505호 (가양동, 한강타운아파트)

【거주국】 KR

【출원언어】 국어

【심사청구】 청구

【이 발명을 지원한 국가연구개발사업】

【과제고유번호】 2710008520

【과제번호】 I1221022

【부처명】 과학기술정보통신부

【과제관리(전문)기관명】 정보통신기획평가원

【연구사업명】 정보보호핵심원천기술개발(R&D)

【연구과제명】 이벤트 기반 실험시스템 구축을 통한 자동차 내·외부 아티팩트 수집 및 통합 분석 기술 개발

【과제수행기관명】 단국대학교 산학협력단

【연구기간】 2024.01.01 ~ 2024.12.31

【이 발명을 지원한 국가연구개발사업】

【과제고유번호】 2710017608

【과제번호】 2021R1A2C2012574

【부처명】 과학기술정보통신부

【과제관리(전문)기관명】 한국연구재단

【연구사업명】 개인기초연구(과기정통부)

【연구과제명】 모바일 플랫폼 기반 차량 포렌식을 위한 효과적/지능적 프레임워크

【과제수행기관명】 단국대학교

【연구기간】 2024.03.01 ~ 2025.02.28

【취지】 위와 같이 특허청장에게 제출합니다.

대리인 특허법인린 (서명 또는 인)

【수수료】

【출원료】 0 면 46,000 원

【가산출원료】 31 면 0 원

【우선권주장료】 0 건 0 원

【심사청구료】 14 항 880,000 원

【합계】 926,000원

【감면사유】 전담조직(50%감면)[1]

【감면후 수수료】 463,000 원

【발명의 설명】

【발명의 명칭】

모바일 장치에서 발생한 이벤트 데이터를 수집하고 저장하는 장치 및 방법 {Apparatus and method for collecting and storing event data from mobile device}

【기술분야】

【0001】모바일 장치에서 발생한 이벤트 데이터를 수집하고 저장하기 위한 기술과 관련된다.

【0002】본 개시는 다음의 연구과제를 통해 도출된 것이다.

【0003】(1) 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업(No. 2021R1A2C2012574, 모바일 플랫폼 기반 차량 포렌식을 위한 효과적/지능적 프레임워크)

【0004】(2) 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구(No. 2022-0-01022, 이벤트 기반 실험시스템 구축을 통한 자동차 내·외부 아티팩트 수집 및 통합 분석 기술 개발)

【발명의 배경이 되는 기술】

【0005】모바일 장치의 사용이 증가함에 따라 모바일 장치 내에 저장된 디지털 데이터의 분석은 범죄 수사의 핵심으로 등장하게 되었다. 현대 사회에서 국내외에서 발생하는 분쟁의 해결에 있어서 직접적인 증거가 요구되는데, 범죄에 활용되

는 다양한 수단이라는 측면에서 증거 자료로서의 모바일 장치의 중요성은 재차 강조될 필요가 있다. 이에 따라, 범죄의 예방 내지 범죄 증명에 필요한 모바일 포렌식의 절차와 기술의 중요성이 전 산업에 걸쳐 부각되고 있다.

【0006】 한편, 안드로이드의 로깅 시스템은, 특정 목적 또는 이벤트에 따라 메인 버퍼, 시스템 버퍼, 크래시(crash) 버퍼, 커널(kernel) 버퍼 등의 링 버퍼들(ring buffers)에 로그 데이터를 저장하고 관리한다.

【0007】 안드로이드가 설치된 모바일 장치에서, 'adb logcat', 'adb bugreport'와 같은 명령어를 활용하여 로그 데이터를 수집하고 분석할 수 있다. 그러나 링 버퍼들은 512KB에서 5MB 정도로 용량이 제한되어 있어 로그 데이터로 버퍼가 가득 찰 경우, 덮어쓰기에 의해 먼저 저장된 로그 데이터부터 소실된다. 또한 링 버퍼는 휘발성으로 기기의 전원이 종료되거나 시스템이 재부팅될 경우 기존에 저장된 모든 로그 데이터가 사라지는 한계를 가지고 있다.

【0008】 버그를 신고(보고)하기 위한 'adb bugreport'를 활용하면 로그 데이터를 비휘발성 ZIP 파일로 저장할 수 있다. 그러나 명령어 'adb bugreport'는 버그 신고(보고)에 중점을 두고 있기 때문에, 디지털 포렌식 관점에서 그리고 보안사고 조사 관점에서 'adb bugreport'는 효과적이지 않다.

【0009】 이에 따라, 디지털 포렌식 관점에서, 그리고 모바일 장치에 대한 사이버 공격 탐지 관점에서, 모바일 장치에서 발생하는 이벤트 데이터를 효과적으로 수집하고 저장하는 새로운 방식이 필요하다.

【발명의 내용】

【해결하고자 하는 과제】

【0010】 모바일 장치에서 발생한 이벤트 데이터를 수집하고 저장하는 장치 및 방법을 제공하는 것을 목적으로 한다.

【과제의 해결 수단】

【0011】 일 양상에 따른 이벤트 데이터 수집 및 저장 장치는, 브로드캐스트 메시지를 감지하여 모바일 장치에서 발생하는 이벤트를 감지하되, 브로드캐스트 메시지가 감지되지 않으면 옵저버, 시스템 서비스, 접근성 서비스 및 로그 버퍼 상태 모니터링 중 적어도 하나를 활용하여 상기 모바일 장치에서 발생하는 이벤트를 감지하는 이벤트 감지부; 상기 이벤트가 감지되면 상기 감지된 이벤트에 대한 이벤트 데이터를 생성하고, 상기 생성된 이벤트 데이터를 로그 버퍼에 임시 저장하는 이벤트 데이터 생성부; 및 상기 이벤트 데이터를 서버가 저장할 수 있도록 상기 로그 버퍼에 임시 저장된 이벤트 데이터를 상기 서버에 전송하는 이벤트 데이터 송신부를 포함한다.

【0012】 상기 모바일 장치에는 안드로이드 운영체제가 설치될 수 있다.

【0013】 상기 브로드캐스트 메시지는 이벤트의 발생을 전파하는 메시지이고, 상기 옵저버는 특정 객체의 상태 변화를 감지하는 객체이고, 상기 시스템 서비스는 특정 하드웨어나 소프트웨어 상태의 변화를 감지하고 그 변화에 따라 작업을 트리거하는 역할을 수행하는 백그라운드 서비스이고, 상기 접근성 서비스는 UI 요소들

을 관찰하고 조작할 수 있는 기능을 제공하는 서비스일 수 있다.

【0014】 상기 브로드캐스트 메시지를 통해 감지되는 이벤트는 부팅, 전원 끄기 또는 재부팅, 타임스탬프 조작, 블루투스 상태, 전화 발신 및 메시지 수신을 포함하고, 상기 옵저버를 통해 감지되는 이벤트는 파일의 생성, 수정 및 삭제, 파일의 메타데이터 수정, 메시지 송신을 포함하고, 상기 시스템 서비스를 통해 감지되는 이벤트는 전화 수신, 통화 연결, 통화 거절, 발신 전화 끊기, 수신 전화 끊기를 포함하고, 상기 접근성 서비스를 통해 감지되는 이벤트는 애플리케이션의 포그라운드로의 전환, UI 요소 클릭을 포함하고, 상기 로그 버퍼 상태 모니터링을 통해 감지되는 이벤트는 로그 버퍼 비우기를 포함할 수 있다.

【0015】 상기 서버는 비휘발성 스토리지를 포함할 수 있다.

【0016】 상기 이벤트 데이터 송신부는 상기 로그 버퍼에 이벤트 데이터가 쌓인 용량이 설정된 임계값에 도달하거나, 로그 버퍼 비우기 명령 실행전, 또는 전원 끄기 또는 재부팅 전에, 상기 이벤트 데이터를 상기 서버에 전송할 수 있다.

【0017】 상기 이벤트 데이터 송신부는 새로운 이벤트 데이터가 생성되어 상기 로그 버퍼에 저장될 때마다 또는 설정된 주기 마다, 상기 이벤트 데이터를 상기 서버에 전송할 수 있다.

【0018】 일 양상에 따른 컴퓨팅 장치에 의해 수행되는 이벤트 데이터 수집 및 저장 방법은, 브로드캐스트 메시지를 감지하여 모바일 장치에서 발생하는 이벤트를 감지하되, 브로드캐스트 메시지가 감지되지 않으면 옵저버, 시스템 서비스,

접근성 서비스 및 로그 버퍼 상태 모니터링 중 적어도 하나를 활용하여 상기 모바일 장치에서 발생하는 이벤트를 감지하는 단계; 상기 이벤트가 감지되면 상기 감지된 이벤트에 대한 이벤트 데이터를 생성하고, 상기 생성된 이벤트 데이터를 로그 버퍼에 임시 저장하는 단계; 및 상기 이벤트 데이터를 서버가 저장할 수 있도록 상기 로그 버퍼에 임시 저장된 이벤트 데이터를 상기 서버에 전송하는 단계를 포함한다.

【0019】 상기 모바일 장치에는 안드로이드 운영체제가 설치될 수 있다.

【0020】 상기 브로드캐스트 메시지는 이벤트의 발생을 전파하는 메시지이고, 상기 옵저버는 특정 객체의 상태 변화를 감지하는 객체이고, 상기 시스템 서비스는 특정 하드웨어나 소프트웨어 상태의 변화를 감지하고 그 변화에 따라 작업을 트리거하는 역할을 수행하는 백그라운드 서비스이고, 상기 접근성 서비스는 UI 요소들을 관찰하고 조작할 수 있는 기능을 제공하는 서비스일 수 있다.

【0021】 상기 브로드캐스트 메시지를 통해 감지되는 이벤트는 부팅, 전원 끄기 또는 재부팅, 타임스탬프 조작, 블루투스 상태, 전화 발신, 메시지 수신을 포함하고, 상기 옵저버를 통해 감지되는 이벤트는 파일의 생성, 수정 및 삭제, 파일의 메타데이터 수정, 메시지 송신을 포함하고, 상기 시스템 서비스를 통해 감지되는 이벤트는 전화 수신, 통화 연결, 통화 거절, 발신 전화 끊기, 수신 전화 끊기를 포함하고, 상기 접근성 서비스를 통해 감지되는 이벤트는 애플리케이션의 포그라운드로의 전환, UI 요소 클릭을 포함하고, 상기 로그 버퍼 상태 모니터링을 통해 감지되는 이벤트는 로그 버퍼 비우기를 포함할 수 있다.

【0022】 상기 서버는 비휘발성 스토리지를 포함할 수 있다.

【0023】 상기 이벤트 데이터를 서버에 전송하는 단계는 상기 로그 버퍼에 이벤트 데이터가 쌓인 용량이 설정된 임계값에 도달하거나, 로그 버퍼 비우기 명령 실행전, 또는 전원 끄기 또는 재부팅 전에, 상기 이벤트 데이터를 상기 서버에 전송할 수 있다.

【0024】 상기 이벤트 데이터를 서버에 전송하는 단계는 새로운 이벤트 데이터가 생성되어 상기 로그 버퍼에 저장될 때마다 또는 설정된 주기 마다, 상기 이벤트 데이터를 상기 서버에 전송할 수 있다.

【발명의 효과】

【0025】 예시적 실시예에 따르면, 브로드캐스트 메시지를 포함한 다양한 방식으로 사용자 행위 관련 이벤트를 감지하고 감지된 이벤트에 대한 이벤트 데이터를 생성하여 비휘발성 스토리지에 저장함으로써, 모바일 장치에 대한 루트 권한이 없어도 다양한 이벤트 데이터를 수집할 수 있다. 또한, 모바일 장치의 로그 버퍼 용량이 부족하거나, 모바일 장치의 전원이 꺼지거나 시스템이 재부팅되는 등 이벤트 데이터 유실 가능성이 있는 다양한 상황에서도 이벤트 데이터를 안전하게 저장할 수 있다. 이를 통해 포렌식 과정에서 이벤트 데이터를 보다 효과적으로 활용할 수 있다.

【도면의 간단한 설명】

【0026】도 1은 예시적 실시예에 따른 이벤트 데이터 저장 시스템을 도시한 블록도이다.

도 2는 이벤트 감지 및 이벤트 데이터 생성의 예를 도시한 도면이다.

도 3은 예시적 실시예에 따른 이벤트 데이터 수집 및 저장 방법을 도시한 흐름도이다.

도 4는 일 실시예에 따른 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도이다.

【발명을 실시하기 위한 구체적인 내용】

【0027】이하, 첨부된 도면을 참조하여 본 개시의 일 실시예를 상세하게 설명한다. 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 개시를 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 개시의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다.

【0028】후술되는 용어들은 본 개시에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

【0029】제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 구성요소들은 용어들에 의해 한정되어서는 안 된다. 용어들은 하나의 구성

요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한 복수의 표현을 포함하고, '포함하다' 또는 '가지다' 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것이 존재함을 지정하려는 것이지, 하나 또는 그 이상의 다른 특징들이나 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

【0030】 또한, 본 명세서에서의 구성부들에 대한 구분은 각 구성부가 담당하는 주 기능별로 구분한 것에 불과하다. 즉, 2개 이상의 구성부가 하나의 구성부로 합쳐지거나 또는 하나의 구성부가 보다 세분화된 기능별로 2개 이상으로 분화되어 구비될 수도 있다. 그리고 구성부 각각은 자신이 담당하는 주기능 이외에도 다른 구성부가 담당하는 기능 중 일부 또는 전부의 기능을 추가적으로 수행할 수도 있으며, 구성부 각각이 담당하는 주기능 중 일부 기능이 다른 구성부에 의해 전담되어 수행될 수도 있다. 각 구성부는 하드웨어 또는 소프트웨어로 구현되거나 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

【0031】 도 1은 예시적 실시예에 따른 이벤트 데이터 저장 시스템을 도시한 블록도이고, 도 2는 이벤트 감지 및 이벤트 데이터 생성의 예를 도시한 도면이다.

【0032】 예시적 실시예에 따른 이벤트 데이터 저장 시스템(100)은 모바일 장치에서 발생하는 이벤트 데이터를 수집하고 모바일 장치의 외부에 존재하는 서버에 저장할 수 있다. 여기서 모바일 장치는 스마트폰, 개인 정보 단말기(PDA), 태블릿 컴퓨터 및 정보 기기 등을 포함할 수 있다. 모바일 장치에는 모바일 장치를 제어하

는 모바일 운영체제(OS)가 설치될 수 있으며, 모바일 운영체제는 안드로이드, iOS, 심비안, 블랙베리 OS, 윈도우 폰, 웹OS, 미고 등을 포함할 수 있다. 이하에서는 설명의 편의를 위해 모바일 장치는 안드로이드가 설치된 스마트폰인 경우를 기준으로 설명하기로 한다.

【0033】 도 1을 참조하면, 예시적 실시예에 따른 이벤트 데이터 저장 시스템(100)은 이벤트 데이터 수집 및 저장 장치(110), 로그 버퍼(120) 및 서버(130)를 포함할 수 있다.

【0034】 이벤트 데이터 수집 및 저장 장치(110)는 모바일 장치에 설치되어, 모바일 장치에서 발생하는 이벤트를 감지하고 감지된 이벤트에 대한 이벤트 데이터를 생성 및 수집할 수 있다. 또한, 이벤트 데이터 수집 및 저장 장치(110)는 수집된 이벤트 데이터를 로그 버퍼(120)에 임시 저장하고, 로그 버퍼(120)에 임시 저장된 이벤트 데이터를 서버(130)에 전송하여 서버(130)에 이벤트 데이터를 저장할 수 있다. 이를 위해 이벤트 데이터 수집 및 저장 장치(110)는 이벤트 감지부(111), 이벤트 데이터 생성부(112) 및 이벤트 데이터 송신부(113)를 포함할 수 있다.

【0035】 이벤트 감지부(111)는 모바일 장치에서 발생하는 이벤트를 감지할 수 있다.

【0036】 이벤트 감지부(111)는 이벤트의 종류에 따라 상이한 방법으로 이벤트를 감지할 수 있다. 예를 들어 모바일 장치에서 발생하는 이벤트는 이벤트 감지 방법에 따라 제1 이벤트, 제2 이벤트, 제3 이벤트, 제4 이벤트 및 제5 이벤트로 구분될 수 있다.

【0037】예시적 실시예에 따르면, 이벤트 감지부(111)는 브로드캐스트(broadcast) 메시지를 감지하여 제1 이벤트를 감지할 수 있다. 여기서 브로드캐스트 메시지는 시스템이나 애플리케이션에서 발생하는 이벤트나 정보를 다른 애플리케이션에 전파하는 메시지일 수 있다. 브로드캐스트 메시지를 통해 감지되는 제1 이벤트는 부팅, 전원 끄기(또는 재부팅), 타임스탬프 조작, 블루투스 상태(예컨대, 연결, 끊김, 스트리밍 등), 전화 발신, 메시지 수신 등을 포함할 수 있으나 이에 한정되는 것은 아니다.

【0038】예시적 실시예에 따르면, 이벤트 감지부(111)는 옵저버를 활용하여 제2 이벤트를 감지할 수 있다. 여기서, 옵저버는 특정 객체(주체)의 상태 변화를 감지하는 객체로서, 예를 들어, FileObserver, ContentObserver 등을 포함할 수 있다. 옵저버를 통해 감지되는 제2 이벤트는 파일의 생성, 수정 및 삭제, 파일의 메타데이터 수정, 메시지 송신 등을 포함할 수 있으나 이에 한정되는 것은 아니다. 예를 들어, 이벤트 감지부(111)는 FileObserver를 이용하여 파일의 생성, 수정 및 삭제를 감지하고, ContentObserver를 이용하여 파일의 메타데이터 수정 및 메시지 송신을 감지할 수 있다.

【0039】예시적 실시예에 따르면, 이벤트 감지부(111)는 시스템 서비스를 활용하여 제3 이벤트를 감지할 수 있다. 여기서, 시스템 서비스는 운영체제의 핵심 시스템 기능을 관리하는 백그라운드 서비스로서, 특정 하드웨어나 소프트웨어 상태의 변화를 감지하고, 그 변화에 따라 적절한 작업을 트리거하는 역할을 수행할 수 있다. 시스템 서비스를 통해 감지되는 제3 이벤트는 전화 수신, 통화 연결, 통화

거절, 발신 전화 끊기, 수신 전화 끊기 등을 포함할 수 있으나 이에 한정되는 것은 아니다. 예를 들어, 이벤트 감지부(111)는 시스템 서비스 중 TelephonyManager API를 이용하여 전화 수신, 통화 연결, 통화 거절, 발신 전화 끊기, 수신 전화 끊기를 감지할 수 있다.

【0040】 예시적 실시예에 따르면, 이벤트 감지부(111)는 접근성(accessibility) 서비스를 활용하여 제4 이벤트를 감지할 수 있다. 여기서 접근성 서비스는 시스템의 UI 요소들을 관찰하고 조작할 수 있는 기능을 제공하며, 특히, 사용자가 기기와 상호작용할 때 발생하는 여러 이벤트를 모니터링할 수 있다. 접근성 서비스를 통해 감지되는 제4 이벤트는 애플리케이션 실행 예컨대, 애플리케이션의 포그라운드로의 전환, UI 요소 클릭 등을 포함할 수 있으나 이에 한정되는 것은 아니다.

【0041】 예시적 실시예에 따르면, 이벤트 감지부(111)는 로그 버퍼(120)의 상태를 모니터링하여 제5 이벤트를 감지할 수 있다. 제5 이벤트는 로그 버퍼 비우기 등을 포함할 수 있으나 이에 한정되는 것은 아니다. 예를 들어, 이벤트 감지부(111)는 주기적으로(예컨대, 5초마다) 로그 버퍼(120)에서 최근 로그 항목(latest log entry)을 확인하고, 최근 로그 항목이 비워져 있으면 로그 버퍼 비우기가 실행되었다고 판단할 수 있고 이를 통해 로그 버퍼 비우기 이벤트를 감지할 수 있다.

【0042】 예시적 실시예에 따르면, 이벤트 감지부(111)는 1차적으로 브로드캐스트 메시지의 발생 여부를 감지하여 이를 통해 제1 이벤트를 감지하고, 브로드캐스트 메시지가 발생하지 않으면 2차적으로 옵저버, 시스템 서비스, 접근성 서비스

및 로그 버퍼(120)의 상태 모니터링 등을 통해 제2 내지 제5 이벤트를 감지할 수 있다.

【0043】 예를 들어, 각 이벤트 별 감지 방법은 하기 표 1 내지 표 5로 나타낼 수 있다.

【0044】 [표 1]

【0045】

이벤트	이벤트 상세	브로드캐스트
부팅	부팅	Intent.ACTION_BOOT_COMPLETED
타임스탬프 조작	날짜	Intent.ACTION_DATE_CHANGED
	시간	Intent.ACTION_TIME_CHANGED
전원 끄기	전원 끄기	Intent.ACTION_SHUTDOWN
블루투스	연결	BluetoothDevice.ACTION_ACL_CONNECTED
	연결 끊김	BluetoothDevice.ACTION_ACL_DISCONNECTED
	스트리밍	BluetoothA2dp.ACTION_PLAYIING_STATE_CHANGED: 스트리밍 상태의 변화 BluetoothA2dp.STATE_PLAYING: Streaming 중 BluetoothA2dp.STATE_NOT_PLAYING: NotStreaming BluetoothDevice.EXTRA_DEVICE - Device INFO
전화	발신	Intent.ACTION_NEW_OUTGOING_CALL
메시지	수신	android.provider.Telephony.SMS_RECEIVED

【0046】 [표 2]

【0047】

이벤트	이벤트 상세	옵저버
파일	생성	FileObserver 1. onEvent() // 변화 감지 2. event == CREATE
	수정	FileObserver 1. onEvent() 2. event == MODIFY
	삭제	FileObserver 1. onEvent() 2. event == DELETE

	수정
	(메타데이터)
		ContentObserver
		1. onChange() // 변화감지
		2. getMediaDetails(uri) // 파일 정보 조회

메시지	발신	1. Contentobserver로 "content://sms" 의 데이터베이스를 감시 2. 메시지가 전송되면 데이터베이스에서 기록된 메시지를 찾아 로그 기록

【0048】[표 3]

【0049】

이벤트	이벤트 상세	시스템 서비스
전화	수신	TelephonyManager.CALL_STATE_RINGING
	통화 연결	TelephonyManager.CALL_STATE_OFFHOOK
	통화 거절	1. TelephonyManager.CALL_STATE_IDLE 2. incomingCallNumber != null
	발신 전화 끊기	1. TelephonyManager.CALL_STATE_IDLE 2. lastDialedNumber != null
	수신 전화 끊기	1. TelephonyManager.CALL_STATE_IDLE 2. incomingCallNumber != null

【0050】[표 4]

【0051】

이벤트	이벤트 상세	접근성 서비스
애플리케이션 실행	포그라운드	1. AccessibilityEvent.TYPE_WINDOW_STATE_CHANGED으로 애플리케이션이 포그라운드로 전환되는 것을 추적 2. getPackageName()을 통해 현재 활성화된 애플리케이션의 패키지 명 기록
	클릭	1. AccessibilityEvent.TYPE_VIEW_CLICKED으로 UI 요소 클릭 추적 2. handleViewClicked()로 UI의 텍스트 클래스명을 추출 3. findTextInNode()로 클릭한 UI에 텍스트가 없다면 다른 노드에서 검색

【0052】[표 5]

【0053】

이벤트	이벤트 상세	로그 버퍼 상태
로그 버퍼 비우기	로그 버퍼 비우기	1. 5초마다 로그 버퍼에서 최근 로그 항목(latest log entry) 확인 2. 최근 로그 항목 확인결과, 비워져있다면 로그 버퍼가 비어 있다고 판단하여 로그 데이터 생성 3. 최근 로그 항목 확인결과, 비워져있지 않다면 로그 버퍼 비우기가 실행되지 않았다고 판단

【0054】이벤트 데이터 생성부(112)는 이벤트가 감지되면, 감지된 이벤트에 대한 이벤트 데이터를 생성하고, 생성된 이벤트 데이터를 로그버퍼(120)에 임시 저장할 수 있다. 예를 들어, 이벤트 데이터 생성부(112)는 도 2에 도시된 바와 같은 이벤트 데이터를 생성할 수 있다.

【0055】이벤트 데이터 송신부(113)는 서버(130)가 이벤트 데이터를 저장할 수 있도록, 로그 버퍼(120)에 저장된 이벤트 데이터를 서버(130)에 전송할 수

있다.

【0056】 예시적 실시예에 따르면, 이벤트 데이터 송신부(113)는 새로운 이벤트 데이터가 생성되어 로그 버퍼(120)에 저장될 때마다 또는 설정된 주기 마다 로그 버퍼(130)에 저장된 이벤트 데이터를 서버(130)에 전송할 수 있다.

【0057】 예시적 실시예에 따르면, 이벤트 데이터 송신부(113)는 로그 버퍼(120)에 이벤트 데이터가 쌓인 용량이 설정된 임계값(예컨대, 512KB)에 도달하거나, 로그 버퍼 비우기 명령 실행전, 또는 전원 끄기 또는 재부팅 전에, 로그 버퍼(120)에 저장된 이벤트 데이터를 서버(130)에 전송할 수 있다. 이때, 임계값은 로그 버퍼(120)의 용량을 고려하여 다양하게 설정될 수 있다.

【0058】 예시적 실시예에 따르면, 이벤트 데이터 송신부(113)와 서버(130)는 Spring Boot를 이용한 통신을 수행할 수 있다. 예를 들어, 이벤트 데이터 송신부(113)는 HTTP/HTTPS(REST API)를 이용하여 서버(130)로 텍스트 기반의 데이터 형식(예컨대, JSON(JavaScript Object Notation) 등)의 이벤트 데이터를 POST 방식으로 전송할 수 있으며, 서버(130)는 Spring Boot가 제공하는 REST(representational state transfer) API 엔드포인트에서 이벤트 데이터를 수신할 수 있다. 이벤트 데이터 송신부(113)는 이벤트 데이터를 서버(130)로 전송할 때, 각 이벤트 데이터의 감지 타입을 JSON 필드로 포함할 수 있다. 이때, 감지 타입은 이벤트를 감지한 방식(예컨대, 브로드캐스트, 옵저버, 시스템 서비스, 접근성 서비스 및 로그 버퍼 상태 모니터링 등)을 나타낼 수 있다.

【0059】 로그 버퍼(120)는 이벤트 데이터 수집 및 저장 장치(110)에서 생성

된 이벤트 데이터를 임시 저장할 수 있다. 로그 버퍼(120)는 휘발성 메모리로 형성될 수 있으며, 하나 이상의 링 버퍼들을 포함할 수 있다.

【0060】 서버(130)는 로그 버퍼(120)에 임시 저장된 이벤트 데이터를 수신하여 저장할 수 있다. 서버(130)는 비휘발성 스토리지, 예를 들어, NAS(network attached storage), SAN(storage area network) 스토리지, 클라우드 스토리지 등을 포함할 수 있다.

【0061】 예시적 실시예에 따르면 전술한 바와 같이 서버(130)는 Spring Boot가 제공하는 REST API 엔드포인트에서 이벤트 데이터를 수신하고, 이벤트 데이터의 감지 타입을 분석하여 감지 타입별로 이벤트 데이터를 구분하여 저장할 수 있다.

【0062】 예시적 실시예에 따른 이벤트 데이터 저장 시스템(100)은 모바일 장치의 루트 권한이 없더라도 브로드캐스트 메시지 이외에 다양한 방식으로 사용자 행위 관련 이벤트를 감지하고 감지된 이벤트에 대한 이벤트 데이터를 생성 및 수집하여 비휘발성 스토리지인 서버(130)에 저장함으로써, 휘발성으로 관리되는 로그 버퍼(120)의 한계를 극복할 수 있으며, 포렌식 수사시 효율 또한 극대화할 수 있다.

【0063】 도 3은 예시적 실시예에 따른 이벤트 데이터 수집 및 저장 방법을 도시한 흐름도이다.

【0064】 도 3의 방법은 도 1의 이벤트 데이터 수집 및 저장 장치(110)에 의해 수행될 수 있다. 도시된 흐름도에서는 이벤트 데이터 수집 및 저장 방법을 복수

개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다.

【0065】 도 3을 참조하면, 단계 310에서, 이벤트 데이터 수집 및 장치는 모바일 장치 내부에 설치되어, 모바일 장치에서 발생하는 이벤트를 감지할 수 있다.

【0066】 예시적 실시예에 따르면, 이벤트 데이터 수집 및 저장 장치는 브로드캐스트(broadcast) 메시지를 감지하여 제1 이벤트를 감지할 수 있다. 예를 들어, 브로드캐스트 메시지를 통해 감지되는 제1 이벤트는 부팅, 전원 끄기(또는 재부팅), 타임스탬프 조작, 블루투스 상태(예컨대, 연결, 끊김, 스트리밍 등), 전화 발신, 메시지 수신 등을 포함할 수 있으나 이에 한정되는 것은 아니다.

【0067】 예시적 실시예에 따르면, 이벤트 데이터 수집 및 저장 장치는 옵저버를 활용하여 제2 이벤트를 감지할 수 있다. 옵저버를 통해 감지되는 제2 이벤트는 파일의 생성, 수정 및 삭제, 파일의 메타데이터 수정, 메시지 송신 등을 포함할 수 있으나 이에 한정되는 것은 아니다.

【0068】 예시적 실시예에 따르면, 이벤트 데이터 수집 및 저장 장치는 시스템 서비스를 활용하여 제3 이벤트를 감지할 수 있다. 시스템 서비스를 통해 감지되는 제3 이벤트는 전화 수신, 통화 연결, 통화 거절, 발신 전화 끊기, 수신 전화 끊기 등을 포함할 수 있으나 이에 한정되는 것은 아니다.

【0069】예시적 실시예에 따르면, 이벤트 데이터 수집 및 저장 장치는 접근성 서비스를 활용하여 제4 이벤트를 감지할 수 있다. 접근성 서비스를 통해 감지되는 제4 이벤트는 애플리케이션 실행 예컨대, 애플리케이션의 포그라운드로의 전환, UI 요소 클릭 등을 포함할 수 있으나 이에 한정되는 것은 아니다.

【0070】예시적 실시예에 따르면, 이벤트 데이터 수집 및 저장 장치는 로그 버퍼 상태를 모니터링하여 제5 이벤트를 감지할 수 있다. 제5 이벤트는 로그 버퍼 비우기 등을 포함할 수 있으나 이에 한정되는 것은 아니다.

【0071】예시적 실시예에 따르면, 이벤트 데이터 수집 및 저장 장치는 1차적으로 브로드캐스트 메시지의 발생 여부를 감지하여 이를 통해 제1 이벤트를 감지하고, 브로드캐스트 메시지가 발생하지 않으면 2차적으로 옵저버, 시스템 서비스, 접근성 서비스 및 로그 버퍼 상태 모니터링 등을 통해 제2 내지 제5 이벤트를 감지할 수 있다.

【0072】단계 320에서, 이벤트 데이터 수집 및 저장 장치는 이벤트가 감지되면, 감지된 이벤트에 대한 이벤트 데이터를 생성하고, 생성된 이벤트 데이터를 로그 버퍼에 임시 저장할 수 있다.

【0073】단계 330에서, 이벤트 데이터 수집 및 저장 장치는 로그 버퍼에 임시 저장된 이벤트 데이터를 서버에 전송할 수 있다. 이때 서버는 비휘발성 스토리지, 예를 들어, NAS(network attached storage), SAN(storage area network) 스토리지, 클라우드 스토리지 등을 포함할 수 있다.

【0074】예시적 실시예에 따르면, 이벤트 데이터 수집 및 저장 장치는 새로운 이벤트 데이터가 생성되어 로그 버퍼에 저장될 때마다 또는 설정된 주기 마다 로그 버퍼에 저장된 이벤트 데이터를 서버에 전송할 수 있다.

【0075】예시적 실시예에 따르면, 이벤트 데이터 수집 및 저장 장치는 로그 버퍼에 이벤트 데이터가 쌓인 용량이 설정된 임계값에 도달하거나, 로그 버퍼 비우기 명령 실행전 또는 전원 끄기 또는 재부팅 전에, 로그 버퍼에 저장된 이벤트 데이터를 서버에 전송할 수 있다.

【0076】예시적 실시예에 따르면, 이벤트 데이터 수집 및 저장 장치는 HTTP/HTTPS(REST API)를 이용하여 서버로 텍스트 기반 데이터 형식의 로그 데이터를 POST 방식으로 전송할 수 있다.

【0077】한편, 서버는 로그 버퍼에 임시 저장된 이벤트 데이터를 수신하여 저장할 수 있다.

【0078】예시적 실시예에 따르면 서버는 Spring Boot가 제공하는 REST API 엔드포인트에서 이벤트 데이터를 수신하고, 이벤트 데이터의 감지 타입을 분석하여 감지 타입별로 로그 데이터를 구분하여 저장할 수 있다.

【0079】도 4는 일 실시예에 따른 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 예시하여 설명하기 위한 블록도이다. 도시된 실시예에서, 각 컴포넌트들은 이하에 기술된 것 이외에 상이한 기능 및 능력을 가질 수 있고, 이하에 기술된 것 이외에도 추가적인 컴포넌트를 포함할 수 있다.

【0080】도시된 컴퓨팅 환경(10)은 컴퓨팅 장치(12)를 포함한다. 컴퓨팅 장치(12)는 일 실시예에 따른 이벤트 데이터 저장 시스템(100) 또는 이벤트 데이터 수집 및 저장 장치(110)에 포함된 하나 이상의 컴포넌트일 수 있다.

【0081】컴퓨팅 장치(12)는 적어도 하나의 프로세서(14), 컴퓨터 판독 가능 저장 매체(16) 및 통신 버스(18)를 포함한다. 프로세서(14)는 컴퓨팅 장치(12)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(14)는 컴퓨터 판독 가능 저장 매체(16)에 저장된 하나 이상의 프로그램들을 실행할 수 있다. 상기 하나 이상의 프로그램들은 하나 이상의 컴퓨터 실행 가능 명령어를 포함할 수 있으며, 상기 컴퓨터 실행 가능 명령어는 프로세서(14)에 의해 실행되는 경우 컴퓨팅 장치(12)로 하여금 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.

【0082】컴퓨터 판독 가능 저장 매체(16)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드, 프로그램 데이터 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(16)에 저장된 프로그램(20)은 프로세서(14)에 의해 실행 가능한 명령어의 집합을 포함한다. 일 실시예에서, 컴퓨터 판독 가능 저장 매체(16)는 메모리(랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적절한 조합), 하나 이상의 자기 디스크 저장 디바이스들, 광학 디스크 저장 디바이스들, 플래시 메모리 디바이스들, 그 밖에 컴퓨팅 장치(12)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.

【0083】통신 버스(18)는 프로세서(14), 컴퓨터 판독 가능 저장 매체(16)를 포함하여 컴퓨팅 장치(12)의 다른 다양한 컴포넌트들을 상호 연결한다.

【0084】컴퓨팅 장치(12)는 또한 하나 이상의 입출력 장치(24)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(22) 및 하나 이상의 네트워크 통신 인터페이스(26)를 포함할 수 있다. 입출력 인터페이스(22) 및 네트워크 통신 인터페이스(26)는 통신 버스(18)에 연결된다. 입출력 장치(24)는 입출력 인터페이스(22)를 통해 컴퓨팅 장치(12)의 다른 컴포넌트들에 연결될 수 있다. 예시적인 입출력 장치(24)는 포인팅 장치(마우스 또는 트랙패드 등), 키보드, 터치 입력 장치(터치패드 또는 터치스크린 등), 음성 또는 소리 입력 장치, 다양한 종류의 센서 장치 및/또는 촬영 장치와 같은 입력 장치, 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다. 예시적인 입출력 장치(24)는 컴퓨팅 장치(12)를 구성하는 일 컴포넌트로서 컴퓨팅 장치(12)의 내부에 포함될 수도 있고, 컴퓨팅 장치(12)와는 구별되는 별개의 장치로 컴퓨팅 장치(12)와 연결될 수도 있다.

【0085】이제까지 본 발명에 대하여 그 바람직한 실시 예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 따라서, 본 발명의 범위는 전술한 실시 예에 한정되지 않고 특허 청구범위에 기재된 내용과 동등한 범위 내에 있는 다양한 실시 형태가 포함되도록 해석되어야 할 것이다.

【부호의 설명】

【0086】100: 이벤트 데이터 저장 시스템

110: 이벤트 데이터 수집 및 저장 장치

120: 로그 버퍼

130: 서버

111: 이벤트 감지부

112: 이벤트 데이터 생성부

113: 이벤트 데이터 송신부

10: 컴퓨팅 환경

12: 컴퓨팅 장치

14: 프로세서

16: 컴퓨터 판독 가능 저장 매체

18: 통신 버스

20: 프로그램

22: 입출력 인터페이스

24: 입출력 장치

26: 네트워크 통신 인터페이스

【청구범위】

【청구항 1】

브로드캐스트 메시지를 감지하여 모바일 장치에서 발생하는 이벤트를 감지하되, 브로드캐스트 메시지가 감지되지 않으면 옵저버, 시스템 서비스, 접근성 서비스 및 로그 버퍼 상태 모니터링 중 적어도 하나를 활용하여 상기 모바일 장치에서 발생하는 이벤트를 감지하는 이벤트 감지부;

상기 이벤트가 감지되면 상기 감지된 이벤트에 대한 이벤트 데이터를 생성하고, 상기 생성된 이벤트 데이터를 로그 버퍼에 임시 저장하는 이벤트 데이터 생성부; 및

상기 이벤트 데이터를 서버가 저장할 수 있도록 상기 로그 버퍼에 임시 저장된 이벤트 데이터를 상기 서버에 전송하는 이벤트 데이터 송신부를 포함하는, 이벤트 데이터 수집 및 저장 장치.

【청구항 2】

청구항 1에 있어서,

상기 모바일 장치에는 안드로이드 운영체제가 설치된, 이벤트 데이터 수집 및 저장 장치.

【청구항 3】

청구항 1에 있어서,

상기 브로드캐스트 메시지는 이벤트의 발생을 전파하는 메시지이고, 상기 옵

저버는 특정 객체의 상태 변화를 감지하는 객체이고, 상기 시스템 서비스는 특정 하드웨어나 소프트웨어 상태의 변화를 감지하고 그 변화에 따라 작업을 트리거하는 역할을 수행하는 백그라운드 서비스이고, 상기 접근성 서비스는 UI 요소들을 관찰하고 조작할 수 있는 기능을 제공하는 서비스인, 이벤트 데이터 수집 및 저장 장치.

【청구항 4】

청구항 1에 있어서,

상기 브로드캐스트 메시지를 통해 감지되는 이벤트는 부팅, 전원 끄기 또는 재부팅, 타임스탬프 조작, 블루투스 상태, 전화 발신 및 메시지 수신을 포함하고,

상기 옵저버를 통해 감지되는 이벤트는 파일의 생성, 수정 및 삭제, 파일의 메타데이터 수정, 메시지 송신을 포함하고,

상기 시스템 서비스를 통해 감지되는 이벤트는 전화 수신, 통화 연결, 통화 거절, 발신 전화 끊기, 수신 전화 끊기를 포함하고,

상기 접근성 서비스를 통해 감지되는 이벤트는 애플리케이션의 포그라운드로의 전환, UI 요소 클릭을 포함하고,

상기 로그 버퍼 상태 모니터링을 통해 감지되는 이벤트는 로그 버퍼 비우기를 포함하는, 이벤트 데이터 수집 및 저장 장치.

【청구항 5】

청구항 1에 있어서,

상기 서버는 비휘발성 스토리지를 포함하는, 이벤트 데이터 수집 및 저장 장치.

【청구항 6】

청구항 1에 있어서,

상기 이벤트 데이터 송신부는 상기 로그 버퍼에 이벤트 데이터가 쌓인 용량이 설정된 임계값에 도달하거나, 로그 버퍼 비우기 명령 실행전, 또는 전원 끄기 또는 재부팅 전에, 상기 이벤트 데이터를 상기 서버에 전송하는, 이벤트 데이터 수집 및 저장 장치.

【청구항 7】

청구항 1에 있어서,

상기 이벤트 데이터 송신부는 새로운 이벤트 데이터가 생성되어 상기 로그 버퍼에 저장될 때마다 또는 설정된 주기 마다, 상기 이벤트 데이터를 상기 서버에 전송하는, 이벤트 데이터 수집 및 저장 장치.

【청구항 8】

컴퓨팅 장치에 의해 수행되는 이벤트 데이터 수집 및 저장 방법에 있어서,

브로드캐스트 메시지를 감지하여 모바일 장치에서 발생하는 이벤트를 감지하되, 브로드캐스트 메시지가 감지되지 않으면 옵저버, 시스템 서비스, 접근성 서비스 및 로그 버퍼 상태 모니터링 중 적어도 하나를 활용하여 상기 모바일 장치에서 발생하는 이벤트를 감지하는 단계;

상기 이벤트가 감지되면 상기 감지된 이벤트에 대한 이벤트 데이터를 생성하고, 상기 생성된 이벤트 데이터를 로그 버퍼에 임시 저장하는 단계; 및

상기 이벤트 데이터를 서버가 저장할 수 있도록 상기 로그 버퍼에 임시 저장된 이벤트 데이터를 상기 서버에 전송하는 단계를 포함하는, 이벤트 데이터 수집 및 저장 방법.

【청구항 9】

청구항 8에 있어서,

상기 모바일 장치에는 안드로이드 운영체제가 설치된, 이벤트 데이터 수집 및 저장 방법.

【청구항 10】

청구항 8에 있어서,

상기 브로드캐스트 메시지는 이벤트의 발생을 전파하는 메시지이고, 상기 옵저버는 특정 객체의 상태 변화를 감지하는 객체이고, 상기 시스템 서비스는 특정 하드웨어나 소프트웨어 상태의 변화를 감지하고 그 변화에 따라 작업을 트리거하는 역할을 수행하는 백그라운드 서비스이고, 상기 접근성 서비스는 UI 요소들을 관찰하고 조작할 수 있는 기능을 제공하는 서비스인, 이벤트 데이터 수집 및 저장 방법.

【청구항 11】

청구항 8에 있어서,

상기 브로드캐스트 메시지를 통해 감지되는 이벤트는 부팅, 전원 끄기 또는 재부팅, 타임스탬프 조작, 블루투스 상태, 전화 발신, 메시지 수신을 포함하고,

상기 옵저버를 통해 감지되는 이벤트는 파일의 생성, 수정 및 삭제, 파일의 메타데이터 수정, 메시지 송신을 포함하고,

상기 시스템 서비스를 통해 감지되는 이벤트는 전화 수신, 통화 연결, 통화 거절, 발신 전화 끊기, 수신 전화 끊기를 포함하고,

상기 접근성 서비스를 통해 감지되는 이벤트는 애플리케이션의 포그라운드로의 전환, UI 요소 클릭을 포함하고,

상기 로그 버퍼 상태 모니터링을 통해 감지되는 이벤트는 로그 버퍼 비우기를 포함하는, 이벤트 데이터 수집 및 저장 방법.

【청구항 12】

청구항 8에 있어서,

상기 서버는 비휘발성 스토리지를 포함하는, 이벤트 데이터 수집 및 저장 방법.

【청구항 13】

청구항 8에 있어서,

상기 이벤트 데이터를 서버에 전송하는 단계는 상기 로그 버퍼에 이벤트 데이터가 쌓인 용량이 설정된 임계값에 도달하거나, 로그 버퍼 비우기 명령 실행전, 또는 전원 끄기 또는 재부팅 전에, 상기 이벤트 데이터를 상기 서버에 전송하는,

이벤트 데이터 수집 및 저장 방법.

【청구항 14】

청구항 8에 있어서,

상기 이벤트 데이터를 서버에 전송하는 단계는 새로운 이벤트 데이터가 생성되어 상기 로그 버퍼에 저장될 때마다 또는 설정된 주기 마다, 상기 이벤트 데이터를 상기 서버에 전송하는, 이벤트 데이터 수집 및 저장 방법.

【요약서】

【요약】

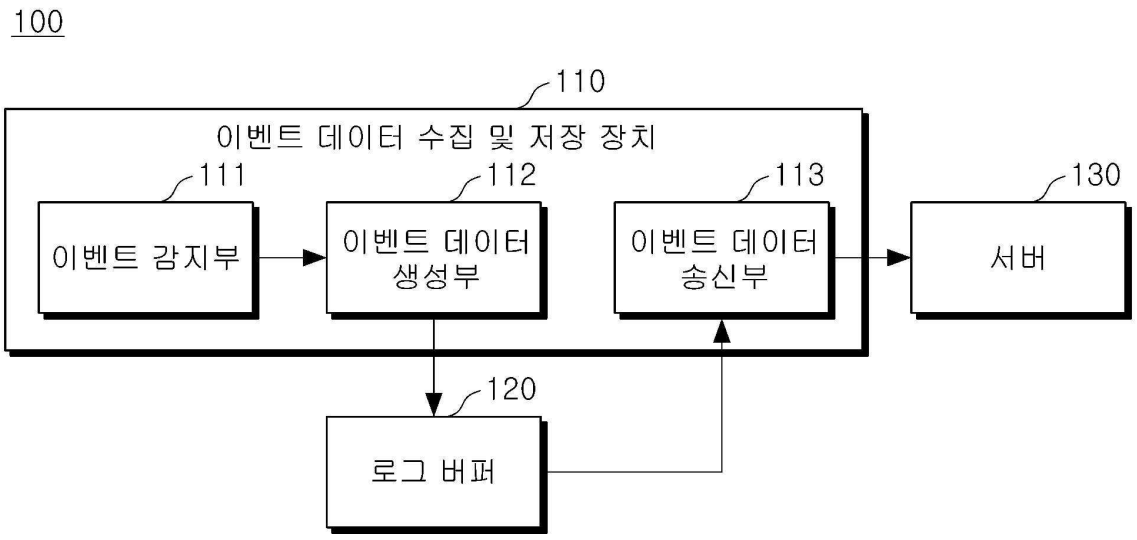
모바일 장치에서 발생한 이벤트 데이터를 수집하고 저장하는 장치 및 방법을 개시한다. 일 실시예에 따른 이벤트 데이터 수집 및 저장 장치는, 브로드캐스트 메시지를 감지하여 모바일 장치에서 발생하는 이벤트를 감지하되, 브로드캐스트 메시지가 감지되지 않으면 옵저버, 시스템 서비스, 접근성 서비스 및 로그 버퍼 상태 모니터링 중 적어도 하나를 활용하여 상기 모바일 장치에서 발생하는 이벤트를 감지하는 이벤트 감지부; 상기 이벤트가 감지되면 상기 감지된 이벤트에 대한 이벤트 데이터를 생성하고, 상기 생성된 이벤트 데이터를 로그 버퍼에 임시 저장하는 이벤트 데이터 생성부; 및 상기 이벤트 데이터를 서버가 저장할 수 있도록 상기 로그 버퍼에 임시 저장된 이벤트 데이터를 사이 서버에 전송하는 이벤트 데이터 송신부를 포함한다.

【대표도】

도 1

【도면】

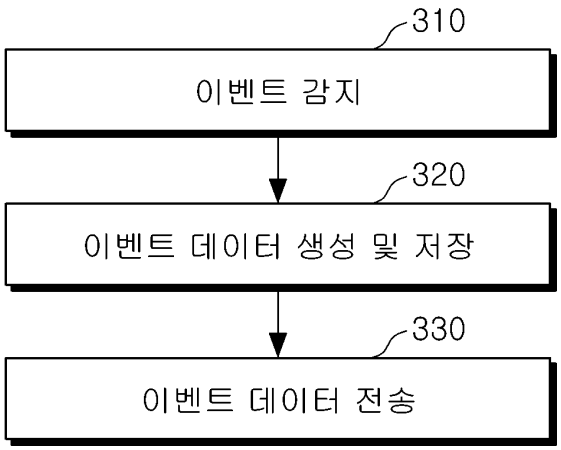
【도 1】


100
110
이벤트 데이터 수집 및 저장 장치
111
이벤트 감지부
112
이벤트 데이터 생성부
113
이벤트 데이터 송신부
130
서버
120
로그 버퍼

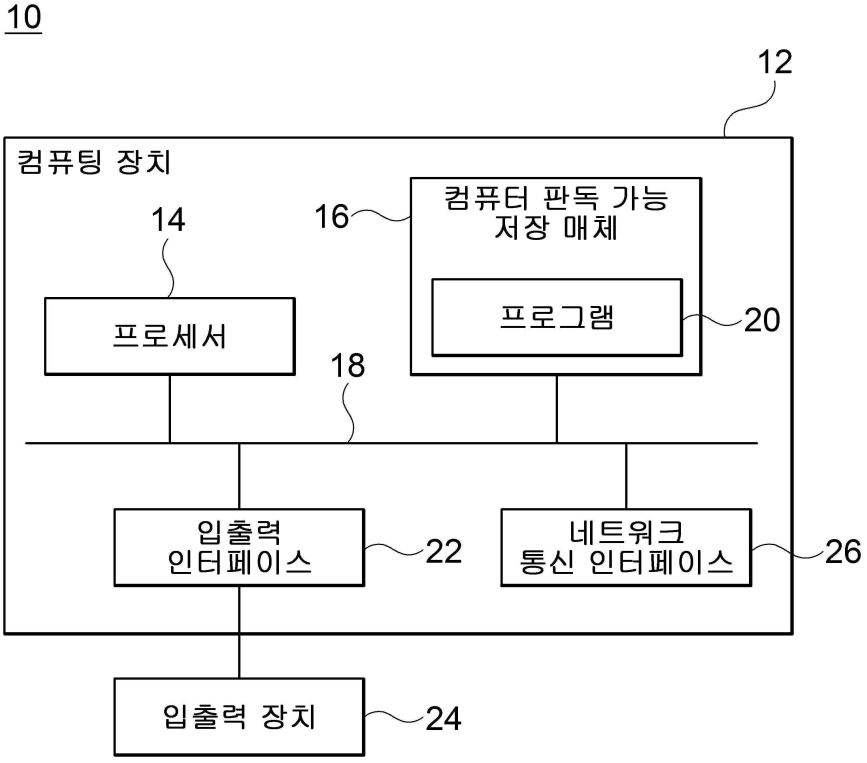
【도 2】

2025-01-07 19:59:40 Call Type: 발신 통화 시작 Number: 01049232198 Start Time: 2025-01-07 19:59:40 End Time: N/A Duration: 0 seconds
2025-01-07 19:59:47 Call Type: 발신 통화 종료 Number: 01049232198 Start Time: 2025-01-07 19:59:40 End Time: 2025-01-07 19:59:47 Duration: 6 seconds
2025-01-07 20:00:04 Call Type: 수신 전화 울림 Number: 01049232198 Start Time: N/A End Time: N/A Duration: 0 seconds
2025-01-07 20:00:07 Call Type: 수신 통화 시작 Number: 01049232198 Start Time: 2025-01-07 20:00:07 End Time: N/A Duration: 0 seconds
2025-01-07 20:00:09 Call Type: 발신 통화 종료 Number: 01049232198 Start Time: 2025-01-07 20:00:07 End Time: 2025-01-07 20:00:09 Duration: 1 seconds
2025-01-07 20:00:39 Call Type: 수신 전화 울림 Number: 01049232198 Start Time: N/A End Time: N/A Duration: 0 seconds
2025-01-07 20:00:42 Call Type: 수신 전화 거절 또는 받지 않음 Number: 01049232198 Start Time: N/A End Time: N/A Duration: 0 seconds
2025-01-07 19:59:03 SMS Sent to/from: 01065749080 Message: TEST
2025-01-07 19:59:03 SMS Received to/from: 01065749080 Message: TEST
2025-01-07 19:59:03 SMS Sent to/from: 01065749080 Message: TEST
2025-01-07 19:59:19 SMS Received to/from: 01065749080 Message: TEST
2025-01-13 22:44:07 Bluetooth connected to: Air Pro 2 [41:42:54:B4:4F:05]
2025-01-13 22:44:07 A2DP streaming stopped on device: Air Pro 2
2025-01-13 22:44:40 A2DP streaming started on device: Air Pro 2
2025-01-13 22:46:02 A2DP streaming stopped on device: Air Pro 2
2025-01-13 22:46:09 Bluetooth disconnected from: null [41:42:54:B4:4F:05]

【도 3】


310
이벤트 감지
320
이벤트 데이터 생성 및 저장
330
이벤트 데이터 전송

【도 4】


10
12
컴퓨팅 장치
14
프로세서
16
컴퓨터 판독 가능
저장 매체
프로그램
20
18
입출력
인터페이스
22
네트워크
통신 인터페이스
26
입출력 장치
24