(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0142782
(43) 공개일자 2014년12월15일

(51) 국제특허분류(Int. Cl.)
G06F 12/16 (2006.01) *G06F 12/14* (2006.01)
(21) 출원번호 10-2013-0063970
(22) 출원일자 2013년06월04일
심사청구일자 2013년06월04일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
대한민국(관리부서 대검찰청)
서울특별시 서초구 반포대로 157 (서초동)
(72) 발명자
이상진
서울 종로구 사직로8길 20, 101동 1503호 (내수동, 파크팰리스)
이인수
서울특별시 용산구 이촌1동 반포아파트 2동 807호
(뒷면에 계속)
(74) 대리인
특허법인충현

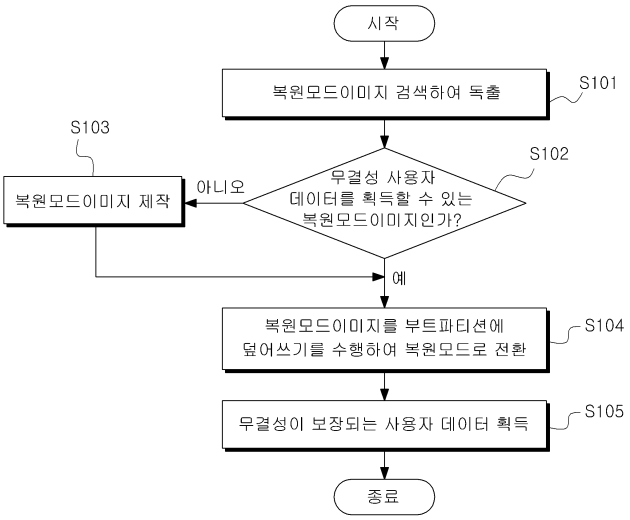
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 **디바이스에서 사용자 데이터의 무결성을 보장하는 데이터 획득 장치 및 방법**

(57) 요 약

디바이스에서 사용자 데이터의 무결성을 보장하는 데이터 획득 장치 및 방법에 관한 것으로, 디바이스에서 사용자 데이터의 무결성을 보장하는 데이터 획득 방법은, 디바이스가 데이터 복구에 가능한 복원모드이미지를 검색하고, 검색된 복원모드이미지를 디바이스가 작동되는 영역인 부트파티션에 덮어쓰기를 수행하여 복원모드로 전환하며, 복원모드로 전환된 디바이스의 사용자 데이터가 기록되어 있는 데이터파티션을 전체 백업 또는 원하는 파일을 선별하여 복사하는 것을 통해 사용자 데이터를 획득한다.

대 표 도 - 도1



(72) 발명자

손남흔

서울 성북구 안암로 145, 정보보호대학원 (안암동 5가, 고려대학교)

김도현

서울 성북구 안암로 145, 정보보호대학원 (안암동 5가, 고려대학교)

이윤호

서울 성북구 안암로 145, 정보보호대학원 (안암동 5가, 고려대학교)

이 발명을 지원한 국가연구개발사업

과제고유번호	2012051106
부처명	교육과학기술부
연구관리전문기관	한국연구재단
연구사업명	원천기술개발사업
연구과제명	대용량 저장장치 조사용 포렌식 시스템 개발
기 여 율	1/1
주관기관	고려대학교 산학협력단
연구기간	2012.10.01 ~ 2013.08.31

특허청구의 범위

청구항 1

디바이스에서 사용자 데이터의 무결성을 보장하는 데이터 획득 방법에 있어서,

상기 디바이스가 무결성을 보장하는 데이터 획득에 이용 가능한 복원모드이미지를 검색하여 독출하는 단계;

상기 독출된 복원모드이미지를 상기 디바이스가 작동되는 영역인 부트파티션(boot partition)에 덮어쓰기를 수행하여 복원모드로 전환하는 단계; 및

상기 복원모드로 전환된 디바이스의 사용자 데이터가 기록되어 있는 데이터파티션(data partition)을 전체 백업 또는 원하는 파일을 선별하여 복사하는 것을 통해 사용자 데이터를 획득하는 단계를 포함하는 방법.

청구항 2

제 1 항에 있어서,

상기 복원모드이미지를 검색하여 독출하는 단계는,

상기 디바이스의 내부 저장매체 또는 네트워크를 통해 연결된 외부 저장매체에 저장된 복원모드이미지를 검색하는 단계;

상기 검색된 복원모드이미지의 소정 영역에 기록된 식별자를 검사함으로써 상기 검색된 복원모드이미지가 무결성을 보장하는 데이터 획득에 이용 가능한 복원모드이미지인지 여부를 판단하는 단계; 및

상기 판단 결과 상기 검색된 복원모드이미지가 무결성을 보장하는 데이터를 획득할 수 있도록 제작되어 있는 경우, 상기 검색된 복원모드이미지를 독출하는 단계를 포함하는 방법.

청구항 3

제 1 항에 있어서,

상기 검색 결과, 무결성을 보장하는 데이터를 획득할 수 있도록 제작되어 있지 않는 경우,

상기 복원모드이미지로부터 램디스크(ramdisk) 영역을 획득하며, 상기 램디스크 영역을 수정하고, 관리자 권한을 활성화함으로써 데이터 획득 시 무결성을 보장하는 복원모드이미지를 제작하는 단계를 더 포함하는 방법.

청구항 4

제 2 항에 있어서,

상기 디바이스는 안드로이드(Android) 모바일 운영 체제 규격에 따른 것으로서,

상기 램디스크 영역은,

상기 복원모드이미지를 분리하여 상기 복원모드이미지를 통해 분리된 piggy.gz 파일을 획득하고,

상기 piggy.gz 파일을 압축 해제하여 상기 piggy.gz 파일을 통해 압축 해제된 ramdisk.cpio 파일을 획득하며,

상기 ramdisk.cpio 파일을 파일 분리하여 상기 ramdisk.cpio 파일을 통해 파일 분리된 램디스크를 획득하는 것을 특징으로 하는 방법.

청구항 5

제 2 항에 있어서,

상기 디바이스는 안드로이드(Android) 모바일 운영 체제 규격에 따른 것으로서,

상기 램디스크는 상기 디바이스의 커널이 동작하는 공간인 루트파일시스템(root file system) 파티션을 읽기/쓰기 모드로 마운트 되도록 수정하는 것을 특징으로 하는 방법.

청구항 6

제 2 항에 있어서,

상기 디바이스는 안드로이드(Android) 모바일 운영 체제 규격에 따른 것으로서,

상기 관리자 권한의 획득은 init.rc 파일을 수정하는 경우, adbd 파일을 수정하는 경우 중 어느 하나인 것을 특징으로 하는 방법.

청구항 7

제 2 항에 있어서,

상기 복원모드이미지는 부트파티션의 최대 용량보다 작게 제작하는 것을 특징으로 하는 방법.

청구항 8

제 1 항에 있어서,

상기 복원모드이미지는 부트헤더(boot header), 커널(kernel) 및 램디스크(ramdisk)를 포함하는 것을 특징으로 하는 방법.

청구항 9

제 1 항에 있어서,

상기 복원모드로 전환하는 단계는,

소정의 파티션 이미지를 안드로이드(Android) 모바일 운영 체제 규격에서 작동 되도록 하는 플래싱모드(flashing mode)에 기초하여 전환하는 것을 특징으로 하는 방법.

청구항 10

제 1 항에 있어서,

상기 원하는 파일을 선별하여 복사하는 것은,

상기 디바이스의 데이터파티션을 읽기전용모드로 마운트 한 뒤 파일 단위로 사용자 데이터를 획득하는 것을 특징으로 하는 방법.

청구항 11

제 1 항에 있어서,

상기 디바이스의 원본 펌웨어 버전을 확인하는 단계;

상기 원본 펌웨어로부터 부트파티션 이미지를 분리하는 단계; 및

상기 부트파티션 이미지를 부트블록에 덮어쓰기를 수행함으로써, 상기 디바이스를 상기 복원모드 이전 상태로 복구하는 단계를 더 포함하는 방법.

청구항 12

제 1 항 내지 제 11 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

청구항 13

사용자 데이터의 무결성을 보장하는 데이터 획득 장치에 있어서,

데이터 복구가 가능한 복원모드이미지를 검사하는 검사부;

상기 검사된 복원모드이미지를 부트파티션에 기록하는 부팅영역 기록부;

상기 부팅영역 기록부에 기록된 이미지에 따라 부팅모드를 수행하는 제어부; 및

상기 제어부에 따라 부팅모드가 복원모드로 부팅될 경우 사용자 데이터가 기록되어 있는 데이터파티션을 전체

백업 또는 원하는 파일을 선별하여 복사하는 것을 통해 사용자 데이터를 획득하는 처리부를 포함하는 장치.

청구항 14

제 13 항에 있어서,

상기 검사부는,

디바이스의 내부 저장매체 또는 네트워크를 통해 연결된 외부 저장매체에 저장된 복원모드이미지를 검색하고,

상기 검색된 복원모드이미지의 소정 영역에 기록된 식별자를 검사함으로써 상기 검색된 복원모드이미지가 무결성을 보장하는 데이터 획득에 이용 가능한 복원모드이미지인지 여부를 판단하며,

상기 판단 결과 상기 검색된 복원모드이미지가 무결성을 보장하는 데이터를 획득할 수 있는 경우, 상기 검색된 복원모드이미지를 독출하게 되고,

상기 검색된 복원모드이미지가 무결성을 보장하는 데이터를 획득할 수 없는 경우, 상기 복원모드이미지를 분리하여 램디스크 영역을 획득하며, 상기 램디스크 영역을 수정하고, 관리자 권한을 활성화함으로써 데이터 획득 시 무결성을 보장하는 복원모드이미지를 제작하는 것을 특징으로 하는 장치.

청구항 15

제 13 항에 있어서,

원하는 파일을 선별하여 복사하는 것을 통해 사용자 데이터를 획득하는 처리부는,

상기 디바이스의 데이터파티션을 읽기전용모드로 마운트 한 뒤 파일 단위로 사용자 데이터를 획득하는 것을 특징으로 하는 장치.

명 세 서

기 술 분 야

[0001] 본 발명은 디바이스에서 무결성을 보장하며 데이터를 획득하는 기술에 관한 것으로, 특히 복원모드의 이미지를 제작하고, 제작된 복원모드이미지를 사용하여 무결성을 보장하는 데이터를 획득하는 장치, 방법 그 방법을 기록한 기록매체에 관한 것이다.

배 경 기 술

[0002] 최근 스마트폰의 등장과 성장에 따라 모바일 소프트웨어 플랫폼에 대한 관심이 증가하고 있다. 또한 안드로이드 폰과 앱스토어의 성공은 스마트폰에서 사용될 애플리케이션에 대한 관심을 한층 끌어올리고 있다. 하지만, 개방형 플랫폼 증가와 앱스토어의 등장으로 인하여 범용 OS를 채택하고 있는 모바일 단말은 모바일 악성코드의 제작을 용이하게 만들고, 제작된 모바일 악성코드는 범용 OS로 인해 이식성이 높기 때문에 모바일 공격의 피해가 증가할 것으로 예상된다. 따라서 향후 지능화되고 다양한 형태로 변형될 수 있는 악성코드 정보 유출, 불법 과금, 부정 사용 등과 같은 보안 위협으로부터 모바일 단말 사용자를 보호하고, 활성화되고 있는 모바일 서비스 환경에 대한 안정성, 무결성, 가용성 및 신뢰성을 제공하기 위한 모바일 서비스 보안 기술이 필요하다.

[0003] 이에 따라 모바일기기의 사용이 증가함에 따라 모바일기기 속에 저장된 디지털 데이터의 분석은 범죄수사의 핵심으로 등장하게 되었고, 현대 사회에서 국내와 국제적으로 발생하는 분쟁의 해결에 있어서 직접적인 증거가 필요하다. 정보통신의 강국이라고 할 수 있는 우리나라에서 사이버 범죄의 유형 통계를 살펴보면 매년 약 10%이상씩 증가하고 있으나, 스마트폰이 출현하는 초기인 2008년은 2007년 대비 약 70% 증가로 최근 급격히 증가 되었다.

[0004] 이와 같이 모바일에 대한 범죄가 급속하게 증가하고 있으므로 관련 범죄의 예방과 이에 따른 범죄 증명에 필요한 모바일 포렌식의 절차와 기술의 중요성이 전 산업에 걸쳐 부각되고 있다.

[0005] 한편, 이하에서 인용되는 선행기술문헌에는 안드로이드의 복원모드를 이용한 데이터 획득 방법을 최초로 소개하였다. 그러나 이러한 기술은 단지 데이터 획득은 가능하나 획득한 데이터의 무결성을 보장하지 못한다는 점에서 일정부분 한계가 존재한다. 만약, 선행기술문헌에 기재된 기술을 활용하여 모바일 포렌식에 적용할 경우 데이터의 무결성이 입증되지 못하여 무용지물이 될 수밖에 없다.

[0006] 이상과 같은 관점에서, 모바일 기기의 사용자 데이터를 복구하여 모바일 포렌식에 사용하기 위해서는 사용자 데이터 복구과정에서 데이터의 무결성을 보장하는 기술적 수단이 필요하다는 사실을 알 수 있다.

선행기술문헌

비특허문헌

[0007] (비특허문헌 0001) (논문문헌 1) 안드로이드의 복원모드를 이용한 데이터 수집방법 {Toward a general collection methodology for Android device}, Digital Investigation Journal, 2011.08.11. 공개.

발명의 내용

해결하려는 과제

[0008] 본 발명이 해결하고자 하는 기술적 과제는, 루팅을 이용하여 디바이스의 데이터를 획득하는 종래의 방식에서 데이터가 훼손되는 영역이 많이 발생한다는 단점을 해결하고, 단순히 복원모드를 이용하여 데이터를 획득하는 방식 역시 여전히 데이터의 무결성을 훼손할 수 있는 다양한 변수가 발생하는 한계를 극복하고자 한다.

과제의 해결 수단

[0009] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 디바이스에서 사용자 데이터의 무결성을 보장하는 데이터 획득 방법에 있어서,

[0010] 상기 디바이스가 무결성을 보장하는 데이터 획득에 이용 가능한 복원모드이미지를 검색하여 독출하는 단계; 상기 독출된 복원모드이미지를 상기 디바이스가 작동되는 영역인 부트파티션(boot partition)에 덮어쓰기를 수행하여 복원모드로 전환하는 단계; 및 상기 복원모드로 전환된 디바이스의 사용자 데이터가 기록되어 있는 데이터파티션(data partition)을 전체 백업 또는 원하는 파일을 선별하여 복사하는 것을 통해 사용자 데이터를 획득하는 단계를 포함한다.

[0011] 일 실시예에 따른 상기 무결성을 보장하는 데이터 획득 방법에서, 상기 복원모드이미지를 검색하여 독출하는 단계는, 상기 디바이스의 내부 저장매체 또는 네트워크를 통해 연결된 외부 저장매체에 저장된 복원모드이미지를 검색하는 단계; 상기 검색된 복원모드이미지의 소정 영역에 기록된 식별자를 검사함으로써 상기 검색된 복원모드이미지가 무결성을 보장하는 데이터 획득에 이용 가능한 복원모드이미지인지 여부를 판단하는 단계; 및 상기 판단 결과 상기 검색된 복원모드이미지가 무결성을 보장하는 데이터를 획득할 수 있도록 제작되어 있는 경우, 상기 검색된 복원모드이미지를 독출하는 단계를 더 포함할 수 있다.

[0012] 일 실시예에 따른 상기 무결성을 보장하는 데이터 획득 방법에서, 상기 검색 결과, 상기 복원모드이미지가 무결성을 보장하는 데이터를 획득할 수 있도록 제작되어 있지 않는 경우, 상기 복원모드이미지로부터 램디스크(ramdisk) 영역을 획득하며, 상기 램디스크 영역을 수정하고, 관리자 권한을 활성화함으로써 데이터 획득 시 무결성을 보장하는 복원모드이미지를 제작하는 단계를 더 포함할 수 있다.

[0013] 일 실시예에 따른 상기 무결성을 보장하는 데이터 획득 방법에서, 상기 원하는 파일을 선별하여 복사하는 것은, 상기 디바이스의 데이터파티션을 읽기전용모드로 마운트 한 뒤 파일 단위로 사용자 데이터를 획득하는 것을 더 포함할 수 있다.

[0014] 한편, 이하에서는 상기 기재된 무결성을 보장하는 데이터 획득 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

[0015] 상기 기술적 과제를 해결하기 위하여, 본 발명의 일 실시예에 따른 사용자 데이터의 무결성을 보장하는 데이터 획득 장치에 있어서, 데이터 복구가 가능한 복원모드이미지를 검사하는 검사부; 상기 검사된 복원모드이미지를 부트파티션에 기록하는 부팅영역 기록부; 상기 부팅영역 기록부에 기록된 이미지에 따라 부팅모드를 수행하는 제어부; 및 상기 제어부에 따라 부팅모드가 복원모드로 부팅될 경우 사용자 데이터가 기록되어 있는 데이터파티션을 전체 백업 또는 원하는 파일을 선별하여 복사하는 것을 통해 사용자 데이터를 획득하는 처리부를 포함한다.

[0016] 일 실시예에 따른 사용자 데이터의 무결성을 보장하는 데이터 획득 장치에서, 상기 검사부는, 디바이스의 내부

저장매체 또는 네트워크를 통해 연결된 외부 저장매체에 저장된 복원모드이미지를 검색하고, 상기 검색된 복원모드이미지의 소정 영역에 기록된 식별자를 검사함으로써 상기 검색된 복원모드이미지가 무결성을 보장하는 데이터 획득에 이용 가능한 복원모드이미지인지 여부를 판단하며, 상기 판단 결과 상기 검색된 복원모드이미지가 무결성을 보장하는 데이터를 획득할 수 있는 경우, 상기 검색된 복원모드이미지를 독출하고, 상기 검색된 복원모드이미지가 무결성을 보장하는 데이터를 획득할 수 없는 경우, 상기 복원모드이미지를 분리하여 램디스크 영역을 획득하며, 상기 램디스크 영역을 수정하고, 관리자 권한을 활성화함으로써 데이터 획득 시 무결성을 보장하는 복원모드이미지를 제작할 수 있다.

[0017] 일 실시예에 따른 사용자 데이터의 무결성을 보장하는 데이터 획득 장치에서, 원하는 파일을 선별하여 복사하는 것을 통해 사용자 데이터를 획득하는 처리부는, 상기 디바이스의 데이터파티션을 읽기전용모드로 마운트 한 뒤 파일 단위로 사용자 데이터를 획득할 수 있다.

발명의 효과

[0018] 본 발명의 실시예들은, 무결성이 보장되는 사용자 데이터를 획득할 수 있도록 복원모드이미지를 제작하며, 제작된 복원모드이미지를 통해 복원모드로 부팅 하여 사용자 데이터를 획득함으로써, 획득한 사용자 데이터의 무결성을 보장하며, 데이터의 훼손 없이 데이터를 획득하기 때문에 실제 수사 환경에 효과적으로 활용될 수 있다.

도면의 간단한 설명

[0019] 도 1은 본 발명의 실시예들이 채택하고 있는 디바이스에서 데이터의 무결성을 보장하는 사용자 데이터 획득 방법을 설명하기 위한 흐름도이다.

도 2는 본 발명의 일 실시예에 따른 안드로이드(Android) 모바일 운영 체제를 채택한 디바이스에서 데이터의 무결성을 보장하는 사용자 데이터 획득 방법을 세부적으로 설명하기 위한 흐름도이다.

도 3은 본 발명의 일 실시예에 따른 디바이스에서 데이터의 무결성을 보장하는 사용자 데이터 획득 장치를 도시한 블록도이다.

도 4는 도 2의 복원모드이미지에 대한 상세 구조를 도시한 도면이다.

도 5는 도 2의 복원모드이미지를 제작하는 단계에 있어서, 램디스크 영역을 획득하는 방법을 예시하여 도시한 도면이다.

도 6은 도 2의 복원모드이미지를 제작하는 단계에 있어서, 디바이스 별 각각의 부트파티션과 리커버리파티션의 용량을 비교하여 도시한 도면이다.

도 7은 도 2의 디바이스의 원본 펌웨어 버전을 확인하는 방법을 예시한 도면이다.

도 8은 도 2의 부트파티션 이미지를 부트블록에 덮어쓰기를 수행하는 단계에 있어서, 안드로이드 모바일 운영 체제를 채택한 디바이스 별 각각의 부트 블록 이름을 예시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0020] 본 발명의 실시예들을 설명하기에 앞서 본 발명의 실시예들이 구현, 활용되는 환경에서 발생하고 있는 문제점을 제시하고, 이에 기초하여 안출된 본 발명의 기본 아이디어를 제시하도록 한다.

[0021] 앞서 지적한 바와 같이, 디바이스의 복원모드를 이용한 데이터 획득 방식의 경우, 획득한 데이터의 무결성이 훼손되어 상기 획득한 데이터를 실제 수사과정에 활용하는 것은 매우 어렵다. 따라서, 본 발명의 실시예들은 무결성이 보장되는 사용자 데이터를 획득할 수 있도록 복원모드이미지를 제작하며, 제작된 복원모드이미지를 통해 복원모드로 부팅 하여 사용자 데이터를 획득함으로써, 획득한 사용자 데이터의 무결성을 보장할 수 있는 기술적 수단을 제안하고자 한다.

[0022] 도 1은 본 발명의 실시예들이 채택하고 있는 디바이스에서 데이터의 무결성을 보장하는 사용자 데이터를 획득하는 기본 아이디어를 도시한 흐름도이다.

[0023] S101단계에서, 디바이스는 무결성을 보장하는 데이터 획득에 이용 가능한 복원모드이미지를 검색하여 독출한다.

[0024] S102단계에서, 디바이스는 상기 S101 단계에서 독출된 복원모드이미지가 데이터의 무결성을 보장할 수 있도록 제작되었는지를 확인한다. 이때, 상기 독출된 복원모드이미지가 무결성을 보장할 수 있도록 제작되었을 경우,

S104 단계로 진행하여, 복원모드이미지를 통해 복원모드로 전환한다.

[0025] 반면, 상기 독출된 복원모드이미지가 무결성을 보장할 수 있도록 제작되어 있지 않을 경우, S103 단계로 진행하여, 무결성을 보장할 수 있도록 복원모드이미지를 제작한다.

[0026] S103단계에서, 디바이스는 무결성을 보장할 수 있도록 복원모드이미지를 제작한다. 이때, 상기 복원모드이미지를 분리하여 램디스크(ramdisk) 영역을 획득하며, 상기 램디스영역을 수정하고, 관리자 권한을 활성화함으로써 데이터 획득 시 무결성을 보장하는 복원모드이미지를 제작하게 된다.

[0027] S104단계에서, 디바이스는 상기 제작된 복원모드이미지를 디바이스가 작동되는 영역인 부트파티션(boot partition)에 덮어쓰기를 수행하여 복원모드로 전환한다.

[0028] S105단계에서, 디바이스는 상기 복원모드로 전환된 디바이스의 사용자 데이터가 기록되어 있는 데이터파티션(data partition)을 전체 백업 또는 원하는 파일을 선별하여 복사하는 것을 통해 무결성이 보장되는 사용자 데이터를 획득한다.

[0029] 이하에서는 첨부된 도면을 참조하여 본 발명의 실시예들을 보다 구체적으로 설명한다. 다만, 하기의 설명 및 첨부된 도면에서 본 발명의 요지를 흐릴 수 있는 공지 기능 또는 구성에 대한 상세한 설명은 생략한다. 또한, 도면 전체에 걸쳐 동일한 구성 요소들은 가능한 한 동일한 도면 부호로 나타내고 있음에 유의하여야 한다.

[0030] 도 2는 본 발명의 실시예에 따른 디바이스에서 데이터의 무결성을 보장하는 사용자 데이터를 획득 방법을 세부적으로 도시한 흐름도로서, 안드로이드 모바일 운영 체제를 채택한 디바이스를 예시하고 있다.

[0031] 이하 본 발명의 실시예는 데이터 무결성에 대한 보장이 필요함으로써, 디바이스의 전원이 인가되지 않았다는 가정하에서 진행된다.

[0032] S201 단계에서, 디바이스의 모델명을 확인한다. 안드로이드 모바일 운영 체제 규격의 디바이스의 경우 디바이스 모델 별 부트파티션 및 리커버리파티션의 크기, 부트블록의 경로명이 틀림으로서, 디바이스 기기의 모델명을 미리 확인하는 것이 바람직하다.

[0033] S202 단계에서, 디바이스는 무결성이 보장되는 데이터 획득에 이용 가능한 복원모드의 이미지를 검색하여 독출한다. 즉, 복원모드이미지를 통해 복원모드로 전환시 복원모드이미지가 데이터 무결성을 보장하지 못하는 경우 데이터 획득 시 데이터의 무결성이 훼손되게 된다, 따라서, 디바이스는 데이터의 무결성을 보장할 수 있도록 제작된 복원모드이미지를 검색하여 독출한다.

[0034] 여기서, 상기 복원모드이미지는 상기 디바이스의 내부 저장매체 또는 네트워크를 통해 연결된 외부 저장매체에 저장되고, 상기 저장된 복원모드이미지는 무결성을 보장하는 데이터를 획득할 수 있도록 제작되어 있는 경우, 상기 복원모드이미지의 기록이 가능한 메모리 영역에 식별자를 지정함으로써, 상기 복원모드이미지가 무결성을 보장하는 데이터를 획득할 수 있도록 제작되어 있지 않는 경우와 구분할 수 있다.

[0035] S203 단계에서, 디바이스는 상기 S203 단계에서 상기 복원모드이미지의 식별자를 검사한다. 이때, 상기 식별자가 확인되었을 경우, S205 단계로 진행하여, 디바이스를 플래싱모드로 전환한다.

[0036] 반면, 상기 복원모드이미지의 부트헤더에 식별자가 없는 경우, S204 단계로 진행하며, 무결성을 보장할 수 있도록 원본 복원모드이미지를 수정하여 새로운 복원모드이미지를 제작한다.

[0037] S204 단계에서, 디바이스는 복원모드이미지를 분리하여 램디스크 영역을 획득하며, 상기 램디스크 영역을 수정하고, 관리자 권한을 활성화함으로써 데이터 획득 시 무결성을 보장하는 복원모드이미지를 제작한다.

[0038] 여기서, 복원모드이미지는 하나의 파일로 구성되어 있으며, 원본 복원모드이미지를 수정해서 새로운 복원모드이미지를 만들기 위해서 상기 원본 복원모드이미지를 영역별로 분리해야 한다. 상기의 복원모드이미지의 영역은 이하에서 도 4를 참조하여 설명하도록 한다.

[0039] 도 4는 본 발명의 일 실시예에 따른 복원모드이미지에 대한 상세 구조를 도시한 도면으로서, 상기 복원모드이미지(32)는 부트헤더(41), 커널(42), 램디스크(43), 세컨드스테이지(44) 의 총 4개의 영역으로 구성될 수 있으며, 상기 데이터 무결성이 보장되는 데이터를 획득하기 위한 복원모드이미지를 만들기 위해서는 상기 램디스크(43) 영역을 획득하여야 한다.

[0040] 여기서, 상기 커널 영역은 무결성을 보장하는 데이터를 획득할 수 있도록 복원모드이미지 제작 시 필요에 따라 수정을 해야 하는 경우도 있으며, 상기 커널 영역을 수정하는 방법은 커널 소스를 획득하여 상기 획득한 커널

소스를 수정 후 상기 커널 영역을 새로 컴파일 하는 것이다. 즉, 무결성이 보장되는 복원모드 이미지를 독출할 수 없으며, 상기 복원모드 이미지의 램디스크 영역(43)만을 독출 가능할 경우, 커널 소스를 독출하여 수정 및 상기 독출된 램디스크 영역(43)과 상기 독출하여 수정된 커널 소스를 함께 컴파일 함으로써, 커널 영역(42)을 획득할 수 있다. 상기 커널 소스는 일반적으로 디바이스 제조사의 오픈소스 홈페이지를 통해 공개되고 있으며, 상기 홈페이지에서 각 디바이스의 버전에 대한 커널 소스를 획득할 수 있다.

[0041] 상기 커널 컴파일을 실행하기 위해서는, 리눅스 운영체제와 defconfig, menuconfig 등의 명령어 사용 시 필요한 설정 정보, 디바이스에 적용 가능한 복원모드이미지를 컴파일 하기 위해 필요한 개발 도구들의 집합인 툴체인(Toolchain)이 필요하며, 상기 커널 컴파일을 실행하기 위해서 필요한 사전 정보들은 상기 오픈소스 홈페이지 내에서 확인할 수 있다. 여기서 툴체인은 임베디드(Embedded) 기기에 많이 사용되는 32-bit 프로세서인 ARM(Advanced RISC Machines Ltd) 아키텍쳐 기반의 EABI(Embedded Application Binary Interface)가 사용될 수 있다.

[0042] 또한, 특정 커널 소스에는 사용자가 임의로 수정한 복원모드이미지의 컴파일을 방지하기 위해 커널 소스의 tcrypt.c 파일 및 fips_integruty.c 파일내부에 램디스크의 시그니처(signature), 크기, 및 해시값(HMAC-SHA256) 등을 검사하는 루틴(routine)이 존재하기 때문에, 상기 루틴을 주석처리 하거나 리턴(return)값을 수정함으로써, 해당 함수를 우회하여 커널 컴파일을 수행할 수 있다.

[0043] 이제, 상기 복원모드이미지를 분리하여 상기 램디스크 영역(43)을 획득한다. 상기의 램디스크 영역(43) 획득하는 방법은 이하에서 도 5를 참조하여 설명하도록 한다.

[0044] 도 5는 도 2의 복원모드이미지 제작 과정에서 복원모드이미지의 램디스크 영역을 획득하는 방법을 예시하여 도시한 도면으로서, 상기 램디스크(43) 영역을 획득하기 위해서는 상기 원본 복원모드이미지(32)를 분리하여 piggy.gz 파일(51)을 획득하고, 상기 piggy.gz 파일(51)을 압축 해제하여 상기 piggy.gz 파일(51)을 통해 압축 해제된 ramdisk.cpio 파일(52)을 획득하며, 상기 ramdisk.cpio 파일(52)을 파일 분리하여 상기 ramdisk.cpio 파일(52)을 통해 파일 분리된 램디스크 영역(43)를 획득한다.

[0045] 이제 도 2로 돌아가 S204 단계를 계속해서 기술하도록 한다.

[0046] 램디스크 영역을 획득하면 복원모드이미지를 이용하여 데이터를 획득할 수 있게 수정하여야 하며, 데이터를 획득할 수 있게 하려면 관리자 권한을 활성화해야 한다. 상기 관리자 권한을 활성화하기 위해서는 init.rc 파일을 수정하거나 adbd 파일을 변경하는 작업이 필요하다.

[0047] 한편, 특정 디바이스에서는 rootfs 파티션을 읽기전용 모드로 마운트를 하는 경우가 있는데, 상기의 읽기전용 모드로 마운트 하는 경우 데이터 획득 후 S214 단계의 디바이스를 이전 상태로 원복하는 과정에 있어서 데이터 무결성이 훼손되기 때문에, 읽기/쓰기 모드로 마운트를 해주도록 램디스크 영역을 수정한다. S207 단계인 복원모드로 전환 후 명령어를 통해 읽기/전용 모드로 마운트를 할 수 있지만, 상기의 명령어를 통한 읽기/전용 모드로 마운트를 할 경우 대부분의 디바이스에서 사용되는 파일시스템인 EXT4의 메타데이터 정보 중 마운트 정보가 변경됨에 따라 데이터의 무결성이 훼손된다.

[0048] 추가로, 기본적으로 복원모드를 사용하는 파티션인 리커버리파티션의 최대 용량은 일반 부팅을 위해 사용되는 파티션인 부트파티션의 최대 용량보다 크다. 따라서, 디바이스 별 파티션 크기를 참고하여 복원모드이미지 제작 시 부트파티션의 최대 용량보다 복원모드이미지의 용량을 작게 제작하여야 한다. 상기의 디바이스 별 파티션 크기는 이하에서 도 6을 참조하여 설명하도록 한다.

[0049] 도 6은 본 발명의 일 실시예에 따른 디바이스 별 각각의 부트파티션과 리커버리파티션의 용량을 비교하여 도시한 도면으로서, 모든 디바이스(61)의 리커버리파티션 최대용량(63)이 부트파티션의 최대용량(62)보다 동일하거나 큰 것을 확인할 수 있다. 따라서, 상기 복원모드이미지 제작 시 도 6을 참조하여 복원모드이미지 최대용량을 부트파티션(62) 보다 작게 제작하는 것이 바람직하다.

[0050] 또한, 상기 복원모드이미지 제작시 효율적인 데이터 수집을 위해 비지박스(busybox)와 같은 바이너리를 추가한다. 디바이스 기본 커널에는 파일 복사 명령어 등이 없음으로, 디바이스 운영체제에서 자주 사용되는 명령어들만 모아서 압축해 놓은 busybox 바이너리를 사용하면 효율적인 데이터 수집을 할 수 있다.

[0051] 이제 도 2로 돌아가 S204 단계 이후의 과정에 대해 기술하도록 한다.

[0052] S205 단계에서, 디바이스는 상기 데이터의 무결성을 보장할 수 있도록 제작된 복원모드이미지를 부트파티션에 덮어쓰기를 수행하기 위해 플래싱모드로 부팅한다. 상기 플래싱모드는 특정 파티션 이미지를 디바이스에 쓸 수

있게 해 주는 기능을 제공한다.

[0053] S206 단계에서, 디바이스는 상기 플래싱모드로 부팅이 완료되면 상기 복원모드이미지를 부트파티션에 덮어쓰기를 수행한다.

[0054] S207 단계에서, 디바이스는 일반모드로 재부팅 하며, 상기 부트파티션에 복원모드이미지가 덮어쓰기 되어 있는 상태임으로 부팅 시 복원모드로 전환된다.

[0055] S208 단계에서, 디바이스는 상기 S204 단계에서 관리자 권한을 획득한 상태이기 때문에 사용자 데이터 획득이 가능하다. 데이터 획득이 가능해지면 상기 디바이스에서 사용하는 사용자 데이터가 기록되어 있는 데이터파티션을 전체 백업 또는 원하는 파일을 선별하여 복사하는 것을 통해 사용자 데이터를 획득할 수 있으며, 상기 사용자 데이터 획득을 위해서는 사용자 데이터파티션의 경로 파악이 필요하고, 상기 데이터파티션의 경로는 기기 별로 상이하다.

[0056] S209 단계에서, 상기 S208 단계의 파일을 선별하여 복사하는 것은 사용자 데이터파티션을 마운트 해야한다. 이때, 상기 데이터파티션을 읽기전용모드로 마운트 해야 데이터의 무결성이 훼손되지 않음으로 반드시 상기 데이터파티션을 읽기전용모드로 마운트 한 뒤 파일 단위로 데이터를 획득한다.

[0057] S210 단계에서, 상기 S208 단계의 데이터파티션을 전체 백업하는 것은 파티션이미징 하는 것으로, 상기 파티션이미징을 위해서는 추가로 외부 SD카드 슬롯에 새로운 SD카드를 삽입하여 이미징을 하는 방법이 있다. 하지만, 상기 SD카드를 이용한 파티션이미징 방법은 상기 SD카드 슬롯이 없는 디바이스에서는 사용하지 못하며, 또한, 상기 데이터파티션을 상기 SD카드로 이미징을 한 뒤에 다시 분석 시스템으로 이미지 파일을 이동이 필요함으로 데이터 획득하는 시간이 오래 걸리는 단점이 있다.

[0058] 따라서, 상기 단점을 보완하기 위해서 상기 S204 단계에서 복원모드이미지 제작 시 추가한 비지박스를 이용하여 usb 를 통해 상기 디바이스와 연결된 저장매체에 상기 데이터파티션의 이미징을 수행함으로써 데이터 획득 시 시간이 오래 걸리는 단점을 보완할 수 있다.

[0059] S211 단계에서, 상기 S209 단계 및 S210 단계를 통해 무결성이 보장되는 데이터 획득이 완료되면, 디바이스를 상기 S201 단계의 디바이스 상태인 복원모드 이전으로 복구 시켜야 한다. 즉, 복원모드이미지를 덮어쓰기 수행하여 변경된 부트파티션을 원본 부트파티션으로 다시 덮어쓰기를 수행하여 디바이스를 원복 시켜야 한다.

[0060] 여기서, 상기 원본 부트파티션을 획득하기 위해서는 상기 S201 단계에서 사용하던 디바이스의 펌웨어 버전을 확인해야 한다. 상기 펌웨어 버전 확인은 도 7의 도면에서 확인할 수 있다. 도 7은 본 발명의 일 실시예에 따른 디바이스의 원본 펌웨어 버전을 확인하는 방법을 예시하여 도시한 도면으로써, 디바이스의 /system/build.prop 파일에서 확인 가능하며, 상기 원본 펌웨어 버전 확인은 이하에서 도 7을 참조하여 설명하도록 한다.

[0061] 도 7은 본 발명의 일 실시예에 따른 디바이스의 원본 펌웨어 버전을 확인하는 방법을 예시한 도면으로서, 디바이스의 /system/build.prop 파일을 cat 명령어로 실행하여 ro.build.version.incremental=UH24 라인을 출력함으로써, 상기 디바이스는 UH24 버전의 펌웨어를 사용하는 것을 확인할 수 있다.

[0062] 이제 다시 도 2로 돌아가 S211 단계 이후의 과정에 대해 기술하도록 한다.

[0063] S212단계에서, 디바이스는 현재 디바이스의 부트파티션이 상기 S211단계에서 확인된 원본 펌웨어의 버전과 동일한지를 비교하여, 동일할 경우는 S214 단계로 진행하여 부트파티션 이미지를 부트블록에 덮어쓰기를 수행한다.

[0064] 반면, 상기 비교결과, 부트 파티션 버전이 동일하지 않을 경우는 S213단계로 진행하여 원본 펌웨어에서 부트파티션 이미지를 분리한다.

[0065] S213단계에서, 디바이스는 상기 211단계에서 확인된 원본 펌웨어 버전과 현재 디바이스의 부트파티션 버전이 동일하지 않을 경우, 상기 원본 펌웨어를 수집하고, 상기 수집된 원본 펌웨어에서 부트파티션을 분리한다.

[0066] S214단계에서, 디바이스는 원본 펌웨어의 부트파티션 이미지가 준비되었으면, adb 명령어를 실행하여 상기 디바이스의 루트디렉터리에 상기 준비된 부트파티션 이미지를 복사하며, 복사된 부트파티션 이미지를 상기 디바이스의 부트 블록에 덮어쓰기 함으로서, 디바이스를 상기 S201단계의 상태로 복구한다.

[0067] 여기서, 상기 부트 블록에 부트파티션 이미지를 덮어쓰기 하기 위해서는 디바이스 별 부트 블록 이름을 확인한 뒤 진행되어야 하며, 이는 이하에서 도 8을 참조하여 설명하도록 한다.

[0068] 도 8은 본 발명의 일 실시예에 따른 디바이스 별 각각의 부트 블록 이름을 도시한 도면으로서, 디바이스의 파티

션은 블록단위로 관리되며 부트 블록은 부트파티션 이미지가 기록되는 블록이다. 여기서, 도 8은 디바이스(81)별 부트 블록 이름(82)을 각각 나타내고 있음으로, 상기 S214단계에서 도 8을 참조하여 진행하는 것이 바람직하다.

[0069] 이제, 도 2의 S215단계에서는 상기 S214단계를 통해 디바이스가 상기 S201단계의 상태로 복원되면, 상기 디바이스의 배터리를 분리하여 보관한다. 잘못된 디바이스 작동으로 인해 전원이 인가되어 사용자 데이터의 무결성을 훼손할 가능성이 있기 때문이다.

[0070] 또한, 상기 S210단계에서 연결한 USB 케이블을 제거 하지 않은 상태로 배터리를 분리하면, 특정 디바이스에서는 배터리를 연결하는 순간 사용자 데이터파티션이 마운트 되어 사용자 데이터가 훼손될 가능성이 있음으로, 반드시 배터리를 분리하기 전에 USB 케이블과의 연결을 제거한 뒤에 배터리를 분리한다.

[0071] 도 3은 본 발명의 일 실시예에 따른 디바이스에서 데이터의 무결성을 보장하는 사용자 데이터 획득 장치를 도시한 블록도로서, 도 1 및 도 2를 통해 제시한 디바이스에서 데이터의 무결성을 보장하는 사용자 데이터 획득 방법과 각각의 구성이 대응되므로, 여기서는 장치의 각 구성에 대한 개요만을 밝히되, 구체적인 설명은 생략한다.

[0072] 무결성 데이터 획득 장치(30)는, 복원모드이미지를 검사하는 검사부(31), 상기 검사된 복원모드이미지를 부트파티션에 기록하는 부팅영역 기록부(33), 상기 부팅영역 기록부(33)에 기록된 이미지에 따라 부팅모드를 선택적으로 수행하는 제어부(34) 및 상기 제어부(34)의 요청에 따라 복원모드로 부팅될 경우 사용자 데이터가 기록되어 있는 데이터파티션을 전체 백업 또는 원하는 파일을 선별하여 복사하는 것을 통해 사용자 데이터를 획득하는 처리부(35)를 포함한다.

[0073] 또한, 상기 검사부(31)는, 디바이스의 내부 저장매체 또는 네트워크를 통해 연결된 외부 저장매체에 저장된 복원모드이미지를 검색하고, 상기 검색된 복원모드이미지의 기록이 가능한 메모리 영역에 기록된 식별자를 검사함으로써 상기 검색된 복원모드이미지가 무결성을 보장하는 데이터 획득에 이용 가능한 복원모드이미지인지 여부를 판단하며, 상기 판단 결과 상기 검색된 복원모드이미지가 무결성을 보장하는 데이터를 획득할 수 있는 경우, 상기 검색된 복원모드이미지를 독출하고, 상기 검색된 복원모드이미지가 무결성을 보장하는 데이터를 획득할 수 없는 경우, 상기 복원모드이미지를 분리하여 램디스크 영역을 획득하며, 상기 램디스크 영역을 수정하고, 관리자 권한을 활성화함으로써 데이터 획득 시 무결성을 보장하는 복원모드이미지를 제작할 수 있다.

[0074] 한편, 사용자 데이터를 획득하는 처리부(35)는, 디바이스의 데이터파티션을 읽기전용모드로 마운트 한 뒤 파일 단위로 사용자 데이터를 획득함으로써, 상기 획득한 데이터의 무결성을 보장할 수 있다.

[0075] 상기된 본 발명의 실시예들에 따르면, 무결성이 보장되는 사용자 데이터를 획득할 수 있도록 복원모드이미지를 제작하며, 제작된 복원모드이미지를 통해 복원모드로 부팅 하여 사용자 데이터를 획득함으로써, 획득한 사용자 데이터의 무결성을 보장하며, 데이터의 훼손 없이 데이터를 획득할 수 있다.

[0076] 또한, 데이터의 무결성을 보장한다는 점에서 실제 수사과정에서 범죄 증명에 필요한 중요한 단서로서 그 활용가치가 높다고 볼 수 있다.

[0077] 한편, 본 발명의 실시예들은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록 장치를 포함한다.

[0078] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현하는 것을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의하여 용이하게 추론될 수 있다.

[0079] 이상에서 본 발명에 대하여 그 다양한 실시예들을 중심으로 살펴보았다. 본 발명에 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. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

부호의 설명

[0080] 30 : 무결성 데이터 획득 장치

31 : 검사부

32 : 복원모드이미지

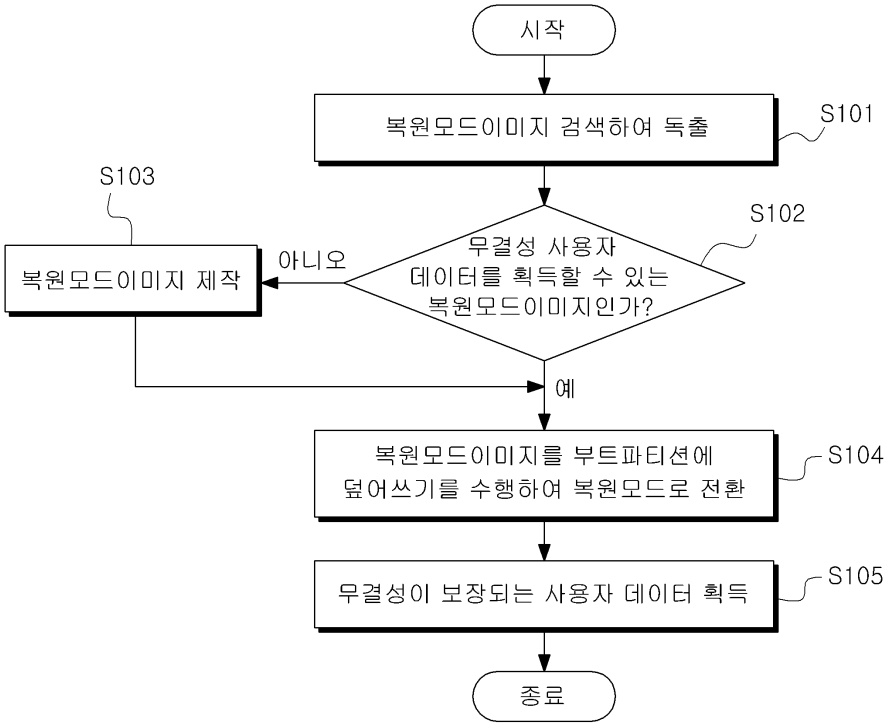
33 : 부팅영역 기록부

33 : 제어부

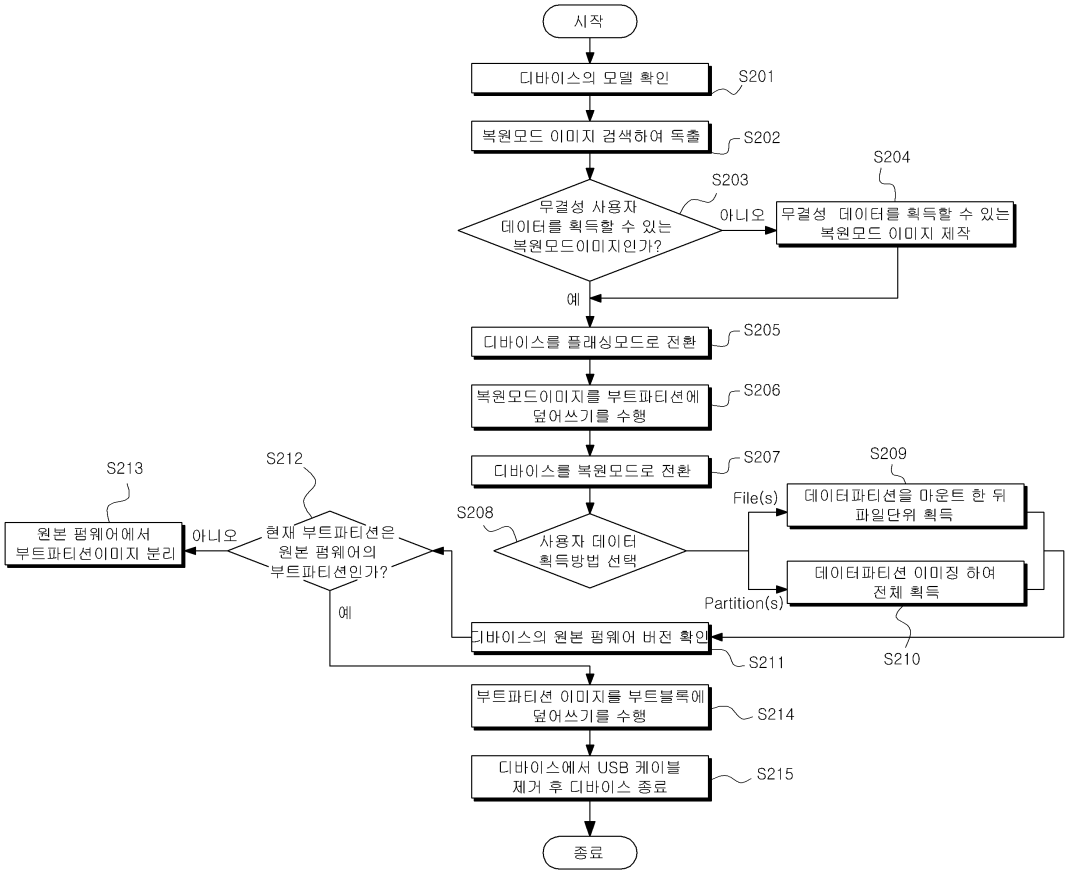
35 : 처리부

도면

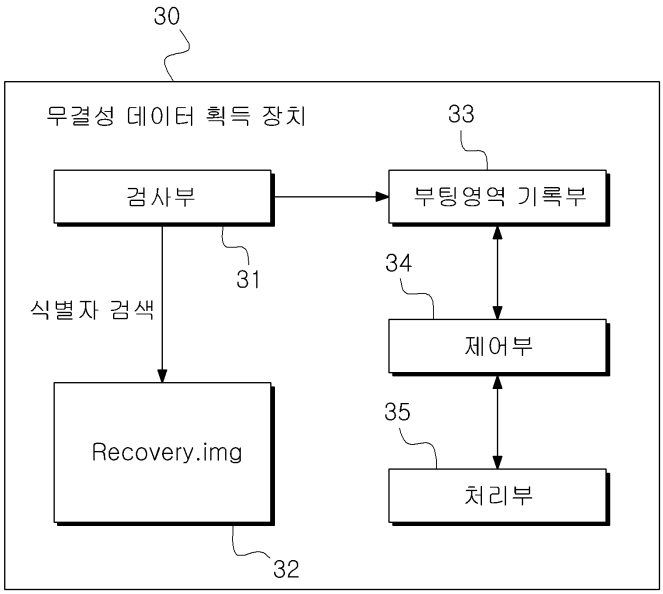
도면1



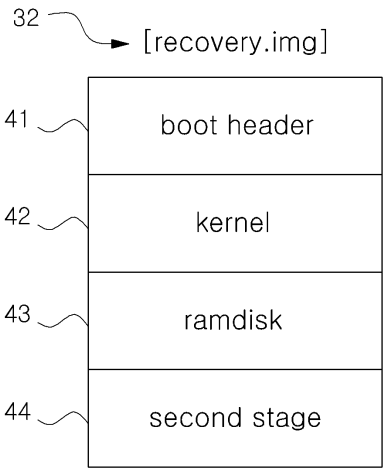
도면2


시작
디바이스의 모델 확인
S201
복원모드 이미지 검색하여 독출
S202
S203
무결성 사용자 데이터를 획득할 수 있는 복원모드이미지인가?
아니오
S204
무결성 데이터를 획득할 수 있는 복원모드 이미지 제작
예
디바이스를 플래싱모드로 전환
S205
복원모드이미지를 부트파티션에 덮어쓰기를 수행
S206
디바이스를 복원모드로 전환
S207
S209
File(s)
데이터파티션을 마운트 한 뒤 파일단위 획득
S208
사용자 데이터 획득방법 선택
데이터파티션 이미징 하여 전체 획득
Partition(s)
S210
S212
현재 부트파티션은 원본 펌웨어의 부트파티션인가?
아니오
S213
원본 펌웨어에서 부트파티션이미지 분리
예
디바이스의 원본 펌웨어 버전 확인
S211
부트파티션 이미지를 부트블록에 덮어쓰기를 수행
S214
디바이스에서 USB 케이블 제거 후 디바이스 종료
S215
종료

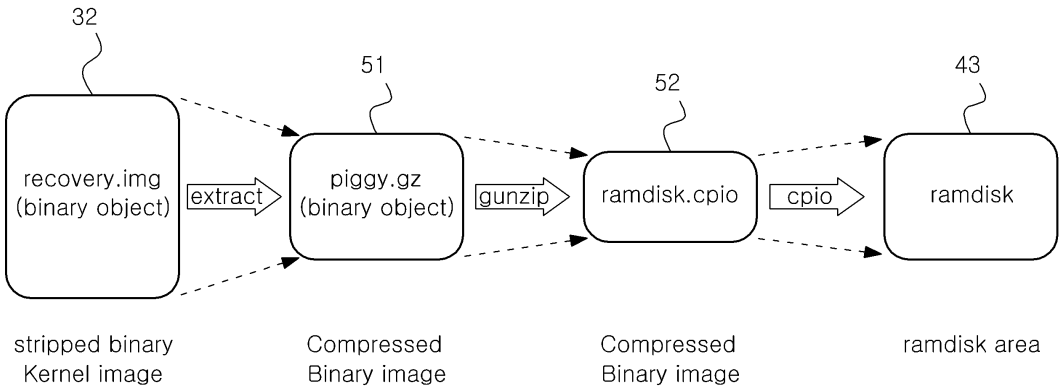
도면3


30
무결성 데이터 획득 장치
33
검사부
부팅영역 기록부
31
34
식별자 검색
제어부
35
Recovery.img
처리부
32

도면4


32
[recovery.img]
41
boot header
42
kernel
43
ramdisk
44
second stage

도면5


32
51
52
43
recovery.img
(binary object)
extract
piggy.gz
(binary object)
gunzip
ramdisk.cpio
cpio
ramdisk
stripped binary
Kernel image
Compressed
Binary image
Compressed
Binary image
ramdisk area

도면6

61 62 63

Device	Size(Kb)	
	Boot Partition	Recovery Partition
Droid (A855)	3584	4608
Galaxy S2 (SHW-M250S)	8192	8192
Galaxy Nexus (SHW-M420K)	8192	12224
Galaxy Note (SHV-E160S)	10240	10240
Galaxy S3 (SHV-E210S)	8192	8192
Galaxy Note 2 (SHV-E250S)	8192	8192
Vega LTE (IM-A800S)	10240	10240

도면7

```
root@android:/ # cat /system/build.prop
cat /system/build.prop
# begin build properties
# autogenerated by buildinfo.sh
ro.build.id=IMM76D
ro.build.display.id=IMM76D.UH24
ro.build.version.incremental=UH24
```

도면8

81 82

Device	Boot block name
Droid (A855)	/dev/block/mtdblock5
Galaxy S2 (SHW-M250S)	/dev/block/mmcblk0p5
Galaxy Nexus (SHW-M420K)	/dev/block/mmcblk0p7
Galaxy Note (SHV-E160S)	/dev/block/mmcblk0p8
Galaxy S3 (SHV-E210S)	/dev/block/mmcblk0p5
Galaxy Note 2 (SHV-E250S)	/dev/block/mmcblk0p8
Vega LTE (IM-A800S)	/dev/block/mmcblk0p8