(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2018-0060838
(43) 공개일자 2018년06월07일

(51) 국제특허분류(Int. Cl.)
G06F 11/36 (2006.01) *G06F 8/40* (2018.01)
(52) CPC특허분류
G06F 11/3628 (2013.01)
G06F 8/41 (2013.01)
(21) 출원번호 10-2016-0160799
(22) 출원일자 2016년11월29일
심사청구일자 없음

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 대학로 99 (궁동, 충남대학교)
(72) 발명자
류재철
대전광역시 유성구 어은로 57, 132동 801호
이서유
경기도 용인시 수지구 죽전로 267, 905동 302호
허혜지
대전광역시 유성구 문화원로37번길 48, 208호
(74) 대리인
홍성욱, 심경식

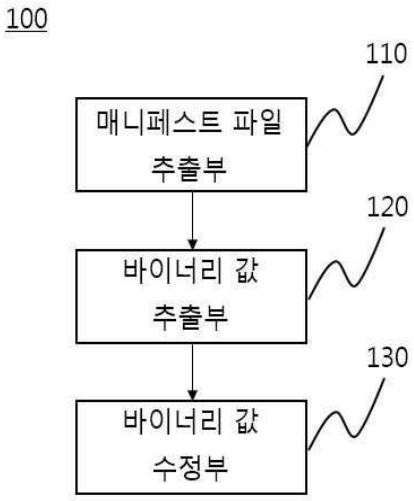
전체 청구항 수 : 총 1 항

(54) 발명의 명칭 **매니페스트 파일 수정 장치 및 방법**

(57) 요 약

안드로이드 어플리케이션(Android Application) 파일의 압축을 해제한 뒤, 매니페스트(Manifest) 파일을 추출하는 매니페스트 파일 추출부, 매니페스트 파일의 내부에서 바이너리(Binary) 값을 추출하는 바이너리 값 추출부 및 디버거블(Debuggable) 스트링의 존재 여부 및 디버거블 스트링의 밸류(Value) 값에 기초하여 추가되는 바이너리 값인 추가 바이너리 값을 바이너리 값에 추가하고, 바이너리 값을 수정하는 바이너리 값 수정부를 포함하는, 매니페스트 파일 수정 장치 및 그 방법에 관한 것이다.

대 표 도 - 도1



(52) CPC특허분류
G06F 8/53 (2013.01)

이 발명을 지원한 국가연구개발사업
과제고유번호 1711035246
부처명 미래창조과학부
연구관리전문기관 정보통신기술진흥센터
연구사업명 대학 ICT 연구센터 육성 지원사업
연구과제명 클라우드 환경의 스마트 기기와 서비스 보안 기술 개발 및 연구 인력양성
기 여 율 1/1
주관기관 숭실대학교 산학협력단
연구기간 2016.01.01 ~ 2016.12.31

명 세 서

청구범위

청구항 1

안드로이드 어플리케이션(Android Application) 파일의 압축을 해제한 뒤, 매니페스트(Manifest) 파일을 추출하는 매니페스트 파일 추출부;

상기 매니페스트 파일의 내부에서 바이너리(Binary) 값을 추출하는 바이너리 값 추출부; 및

디버거블(Debuggable) 스트링의 존재 여부 및 상기 디버거블 스트링의 밸류(Value) 값에 기초하여 추가되는 바이너리 값인 추가 바이너리 값을 상기 바이너리 값에 추가하고, 상기 바이너리 값을 수정하는 바이너리 값 수정부를 포함하는, 매니페스트 파일 수정 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 어플리케이션의 디버깅 모드 활성화를 위해 매니페스트 파일을 수정하는 매니페스트 파일 수정 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 통신기술이 발전함에 따라서, 스마트 폰, 스마트 패드, 각종 웨어러블 디바이스를 비롯한 각종 스마트 기기들이 널리 보급되고 사용되게 되었으며, 이러한 스마트 기기들은 별도로 설치되는 어플리케이션을 통해 각종 기능들을 사용자에게 제공한다.

[0003] 스마트 기기들 중 특히나 안드로이드(Android)에 기반한 스마트 기기들에 설치되는 안드로이드 어플리케이션을 동적 분석하기 위해서는 우선 안드로이드 어플리케이션의 디버깅 모드(Debugging Mode)가 활성화되어 있어야 한다.

[0004] 그러나, 안드로이드 어플리케이션은 기본적으로 디버깅 모드가 비활성화되어 있기 때문에, 안드로이드 어플리케이션을 동적 분석하기 위해서는 안드로이드 어플리케이션을 수정하여 디버깅이 가능한 상태로 변경하여야 한다.

[0005] 이를 위해, 안드로이드 어플리케이션의 설정 파일인 매니페스트 파일(AndroidManifest.xml) 파일을 수정하여야 하는데, 여기서 매니페스트 파일은 인코딩이되어 있으므로, 어플리케이션 디컴파일 과정을 통해 원본 파일을 추출해야 한다.

[0006] 그러나, 실제로 안드로이드 어플리케이션을 동적 분석하기 위해 디버깅 모드를 활성화 시키기 위한 디컴파일 과정에서, 디컴파일 문제로 인해 안드로이드 매니페스트 파일을 수정하기 어려운 경우가 발생할 수 있다.

[0007] 예를 들어, 안드로이드 매니페스트 파일은 인코딩 된 상태로 어플리케이션 내에 저장되어 있고, 이는 디컴파일이 되지 않으면 xml 형태로 확인을 할 수 없으며, 그로 인해 디버깅을 활성화하는 코드를 삽입하는데 어려움이 발생하는 문제가 있다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 한국 공개특허공보 제10-2009-0038894호(2009.04.21)

발명의 내용

해결하려는 과제

[0009] 본 발명의 목적은, 상기 문제점을 해결하기 위한 것으로 매니페스트 파일의 내부에서 바이너리(Binary) 값을 추출한 뒤, 디버거블(Debuggable) 스트링의 존재 여부 및 디버거블 스트링의 밸류(Value) 값에 기초하여 추가되는 바이너리 값인 추가 바이너리 값을 바이너리 값에 추가하고, 바이너리 값을 수정하여, 디컴파일 과정을 생략하고 디버깅 모드를 활성화 시키기 위한 것이다.

[0010] 본 발명이 해결하고자 하는 과제는 이상에서 언급한 과제(들)로 제한되지 않으며, 언급되지 않은 또 다른 과제(들)은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0011] 상기한 목적을 달성하기 위하여, 본 발명의 실시예에 따른 매니페스트 파일 수정 장치는, 안드로이드 어플리케이션(Android Application) 파일의 압축을 해제한 뒤, 매니페스트(Manifest) 파일을 추출하는 매니페스트 파일 추출부, 매니페스트 파일의 내부에서 바이너리(Binary) 값을 추출하는 바이너리 값 추출부 및 디버거블(Debuggable) 스트링의 존재 여부 및 디버거블 스트링의 밸류(Value) 값에 기초하여 추가되는 바이너리 값인 추가 바이너리 값을 바이너리 값에 추가하고, 바이너리 값을 수정하는 바이너리 값 수정부를 포함한다.

발명의 효과

[0012] 본 발명의 일 실시예에 따르면, 매니페스트 파일의 내부에서 바이너리(Binary) 값을 추출한 뒤, 디버거블(Debuggable) 스트링의 존재 여부 및 디버거블 스트링의 밸류(Value) 값에 기초하여 추가되는 바이너리 값인 추가 바이너리 값을 바이너리 값에 추가하고, 바이너리 값을 수정하여, 디컴파일 과정을 생략하고 디버깅 모드를 활성화 시켜 디컴파일 과정에서 생기는 에러를 배제한 채 동적 분석이 가능하다.

도면의 간단한 설명

[0013] 도 1은 본 발명의 실시예에 따른 매니페스트 파일 수정 장치를 설명하기 위한 구성도이다.

도 2는 안드로이드 매니페스트 파일의 구조를 설명하기 위한 도면이다.

도 3은 본 발명의 실시예에 따른 매니페스트 파일 수정 장치 및 방법에서 디버거블 스트링(Debuggable String)이 존재하고 그 밸류(Value) 값이 False로 되어 있는 경우를 설명하기 위한 도면이다.

도 4는 본 발명의 실시예에 따른 매니페스트 파일 수정 장치 및 방법에서 디버거블 스트링(Debuggable String)이 존재하지 않는 경우를 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0014] 이하, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 정도로 상세히 설명하기 위하여, 본 발명의 가장 바람직한 실시예를 첨부 도면을 참조하여 설명하기로 한다. 우선 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다. 또한, 본 발명을 설명함에 있어, 관련된 공지 구성 또는 기능에 대한 구체적인 설명이 본 발명의 요지를 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명은 생략한다.

[0015] 이하, 본 발명의 실시예에 따른 매니페스트 파일 수정 장치 및 방법을 첨부된 도면을 참조하여 상세하게 설명하면 아래와 같다.

[0016] 도 1은 본 발명의 실시예에 따른 매니페스트 파일 수정 장치를 설명하기 위한 구성도이다. 도 2는 안드로이드 매니페스트 파일의 구조를 설명하기 위한 도면이다. 도 3은 본 발명의 실시예에 따른 매니페스트 파일 수정 장치 및 방법에서 디버거블 스트링(Debuggable String)이 존재하고 그 밸류(Value) 값이 False로 되어 있는 경우를 설명하기 위한 도면이다. 도 4는 본 발명의 실시예에 따른 매니페스트 파일 수정 장치 및 방법에서 디버거블 스트링(Debuggable String)이 존재하지 않는 경우를 설명하기 위한 도면이다.

[0017] 도 1에 도시된 바와 같이, 본 발명의 실시예에 따른 매니페스트 파일 수정 장치(100)는 매니페스트 파일 추출부(110), 바이너리 값 추출부(120) 및 바이너리 값 수정부(130)를 포함한다.

[0018] 매니페스트 파일 추출부(110)는 안드로이드 어플리케이션(Android Application) 파일의 압축을 해제한 뒤, 매니페스트(Manifest) 파일을 추출한다.

[0019] 바이너리 값 추출부(120)는 매니페스트 파일의 내부에서 바이너리(Binary) 값을 추출한다.

[0020] 바이너리 값 수정부(130)는 디버거블(Debuggable) 스트링의 존재 여부 및 디버거블 스트링의 밸류(Value) 값에 기초하여 추가되는 바이너리 값인 추가 바이너리 값을 바이너리 값에 추가하고, 바이너리 값을 수정한다.

[0021] 예컨대, 디버거블 스트링(Debuggable String)이 존재하고 그 밸류(Value) 값이 False로 되어 있는 경우에서 바이너리 값 수정부(130)의 동작은 이하 도 3을 참조하여 후술하며, 디버거블 스트링(Debuggable String)이 존재하지 않는 경우에서 바이너리 값 수정부(130)의 동작은 이하 도 4를 참조하여 후술하도록 하며, 중복되는 설명은 생략한다.

[0022] 예컨대, 본 발명의 실시예에 따른 매니페스트 파일 수정 장치(100)는 안드로이드 어플리케이션을 동적 분석하기 위하여 안드로이드 매니페스트 파일을 수정하여 어플리케이션의 디버깅 모드를 활성화 시키는 장치이되, 디컴파일을 통해 매니페스트 파일을 디코딩하는 경우에서 발생하는 에러를 방지하기 위하여, 디컴파일 과정을 생략하고 디버깅 모드를 활성화 시키는 매니페스트 파일 수정 장치(100)를 의미할 수 있다.

[0023] 예를 들어, 본 발명의 실시예에 따른 매니페스트 파일 수정 장치(100) 및 방법은 어플리케이션 디컴파일 과정을 생략하고 인코딩된 안드로이드 매니페스트 파일의 바이너리 값을 추가 및 수정하는 방법을 이용하여 디버깅 모드를 활성화할 수 있다.

[0024] 도 2에 도시된 바와 같이, 안드로이드 매니페스트 파일은 각각의 블록에 AndroidManifest.xml을 구성하는 바이너리 값이 삽입될 수 있으며, String Chunk에는 매니페스트 파일에서 사용되는 모든 스트링 값들이 저장되어 있고, Resource Chunk에는 스트링의 리소스 값들이 저장되며, 각각의 스트링들은 그 속성들이 Tag Chunk내에 존재할 수 있다.

[0025] 예컨대, 본 발명의 실시예에 따른 매니페스트 파일 수정 장치(100) 및 방법은 디버깅 모드를 활성화시키기 위하여 해당되는 값들을 찾아 디버깅 모드를 활성화 시킬 수 있는 바이너리 값을 추가한 뒤, 추가함으로써 발생하는 변경점에 따라 나머지 바이너리 값들을 수정할 수 있다.

[0026] 예컨대, 안드로이드 어플리케이션 파일(패키지 파일로 확장자는 'apk')은 압축파일 형태로 압축을 풀면 패키지 내 파일을 추출할 수 있으며, 본 발명의 실시예에 따른 매니페스트 파일 수정 장치(100) 및 방법은 패키지 파일의 압축을 해제한 후, 매니페스트 파일을 추출하고, 파일 내부의 바이너리 값을 탐색한 뒤 디버깅 모드를 활성화 할 수 있다.

[0027] 이때, 디버깅 모드를 활성화하는 방법은 디버거블 스트링(Debuggable String)이 존재하고 그 밸류(Value) 값이 False로 되어 있는 경우, 디버거블 스트링(Debuggable String)이 존재하지 않는 경우에 따라 각기 달리 동작할 수 있다.

[0028] 도 3에 도시된 바와 같이, 디버거블 스트링(Debuggable String)이 존재하고 그 밸류(Value) 값이 False로 되어 있는 경우에서 바이너리 값 수정부(130)는 디버거블 스트링의 번호와 어플리케이션 스트링의 번호를 추출할 수 있다.

[0029] 여기서, 디버거블 스트링의 경우 어플리케이션 태그(Application Tag) 아래에 위치하는 Attribute Chunk 내에 존재하며, 어플리케이션 태그는 Tag Chunk에 각각의 어플리케이션 스트링의 번호를 가지고 존재한다.

[0030] 이때, 바이너리 값 수정부(130)는 어플리케이션 태그를 찾은 뒤, Attribute Chunk 중 디버거블 스트링의 번호를 포함하는 Attribute Chunk의 밸류 값을 FFFF로 수정하여 디버깅 모드를 활성할 수 있다.

[0031] 도 4에 도시된 바와 같이, 디버거블 스트링(Debuggable String)이 존재하지 않는 경우에서 바이너리 값 수정부(130)는 매니페스트 파일을 전체적으로 수정한다.

[0032] 이 경우, 바이너리 값 수정부(130)는 Header Chunk에서 파일의 크기를 정의한 바이너리 값을 수정할 수 있으며, 수정된 바이너리 값은 "전체 파일 크기 + 추가할 바이너리 크기"일 수 있다.

[0033] 이 경우, 바이너리 값 수정부(130)는 String Chunk에서 스트링 개수를 정의한 바이너리 값을 수정할 수 있으며, 수정된 바이너리 값은 디버거블 스트링을 하나 추가하므로 "전체 스트링 개수 + 1" 일수 있다.

[0034] 이 경우, 바이너리 값 수정부(130)는 String Chunk에 디버거블 스트링을 추가하며, 디버거블 스트링의 주소와 디버거블 스트링을 정의하는 블록을 추가할 수 있으며, 이들은 String Chunk에 삽입되어야 하며, 스트링 중간에 추가하기 위해서는 디버거블 스트링이 추가된 이후의 다른 스트링의 주소를 수정할 수 있다.

[0035] 이 경우, 바이너리 값 수정부(130)는 Resource Chunk에서 디버거블에 해당하는 리소스값을 추가할 수 있으며, 리소스 값을 추가하기 위하여 이전과 이후의 리소스 값의 관계를 분석하여 디버거블 스트링이 추가된 위치의 전후 값들 사이에 추가할 수 있다.

[0036] 이 경우, 바이너리 값 수정부(130)는 Tag Chunk의 어플리케이션 태그 내에 디버거블 스트링을 추가할 수 있으며, 어플리케이션 태그를 찾으면 디버거블의 밸류 값을 정의하는 바이너리 값을 디버거블 스트링의 위치를 고려하여 삽입할 수 있다.

[0037] 이 경우, 바이너리 값 수정부(130)는 디버거블의 추가로 인해 번호가 하나씩 밀린 스트링들을 이용하는 청크들의 해당 부분을 수정하여 안드로이드 매니페스트 파일의 수정을 완료할 수 있다.

[0038] 다시 말해, 본 발명의 실시예에 따른 매니페스트 파일 수정 장치(100) 및 방법은 어플리케이션을 동적 분석하기 위하여 기존에 필요한 디컴파일 과정을 생략하고 인코딩된 매니페스트 파일의 바이너리를 직접 수정하기 때문에 디컴파일이 불가능한 어플리케이션에서도 활용이 가능할 수 있다.

[0039] 즉, 본 발명의 실시예에 따른 매니페스트 파일 수정 장치(100) 및 방법은 디컴파일이 되지 않는 어플리케이션을 비롯하여 동적 분석을 하고자 하는 모든 어플리케이션을 대상으로 활용이 가능할 수 있다.

[0040] 이상에서 본 발명에 따른 바람직한 실시예에 대해 설명하였으나, 다양한 형태로 변형이 가능하며, 본 기술분야에서 통상의 지식을 가진 자라면 본 발명의 특허청구범위를 벗어남이 없이 다양한 변형예 및 수정예를 실시할 수 있을 것으로 이해된다.

부호의 설명

[0041] 100: 매니페스트 파일 수정 장치

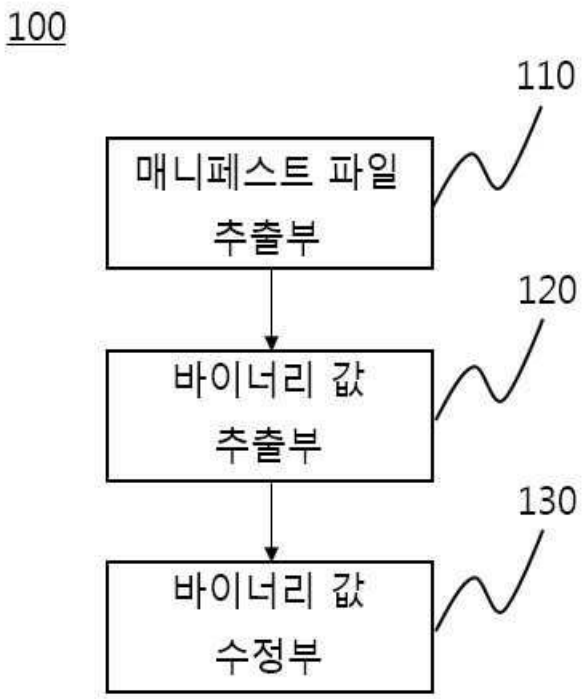
110: 매니페스트 파일 추출부

120: 바이너리 값 추출부

130: 바이너리 값 수정부

도면

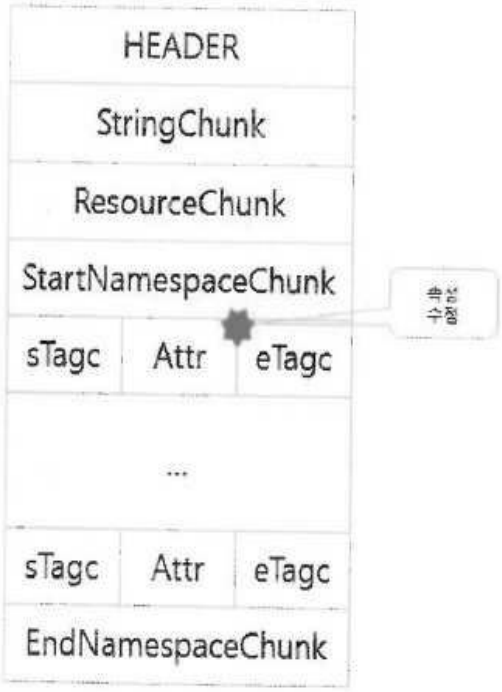
도면1



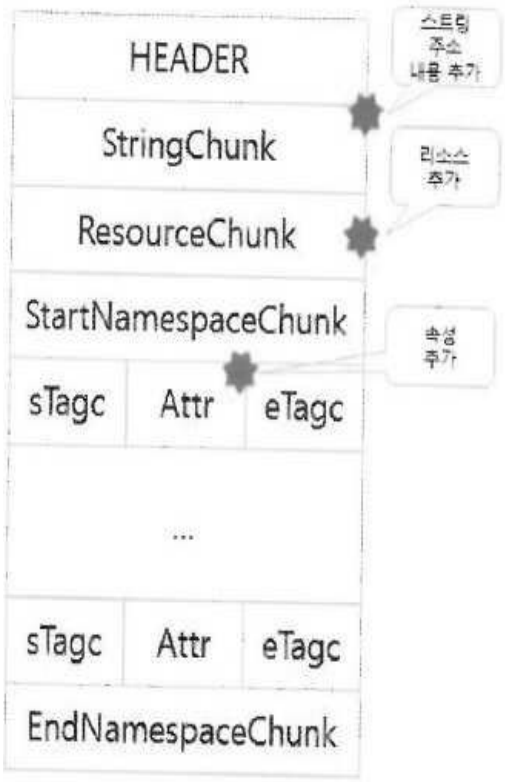
도면2


HEADER
StringChunk
ResourceChunk
StartNamespaceChunk
sTagc
Attr
eTagc
...
sTagc
Attr
eTagc
EndNamespaceChunk

도면3


HEADER
StringChunk
ResourceChunk
StartNamespaceChunk
sTagc
Attr
eTagc
...
sTagc
Attr
eTagc
EndNamespaceChunk

도면4


HEADER
StringChunk
ResourceChunk
StartNamespaceChunk
sTagc
Attr
eTagc
...
sTagc
Attr
eTagc
EndNamespaceChunk
스트링 주소 내용 추가
리소스 추가
속성 추가