APK Hooking

with CydiaSubstrate Framework

namdaehyeon

Goal

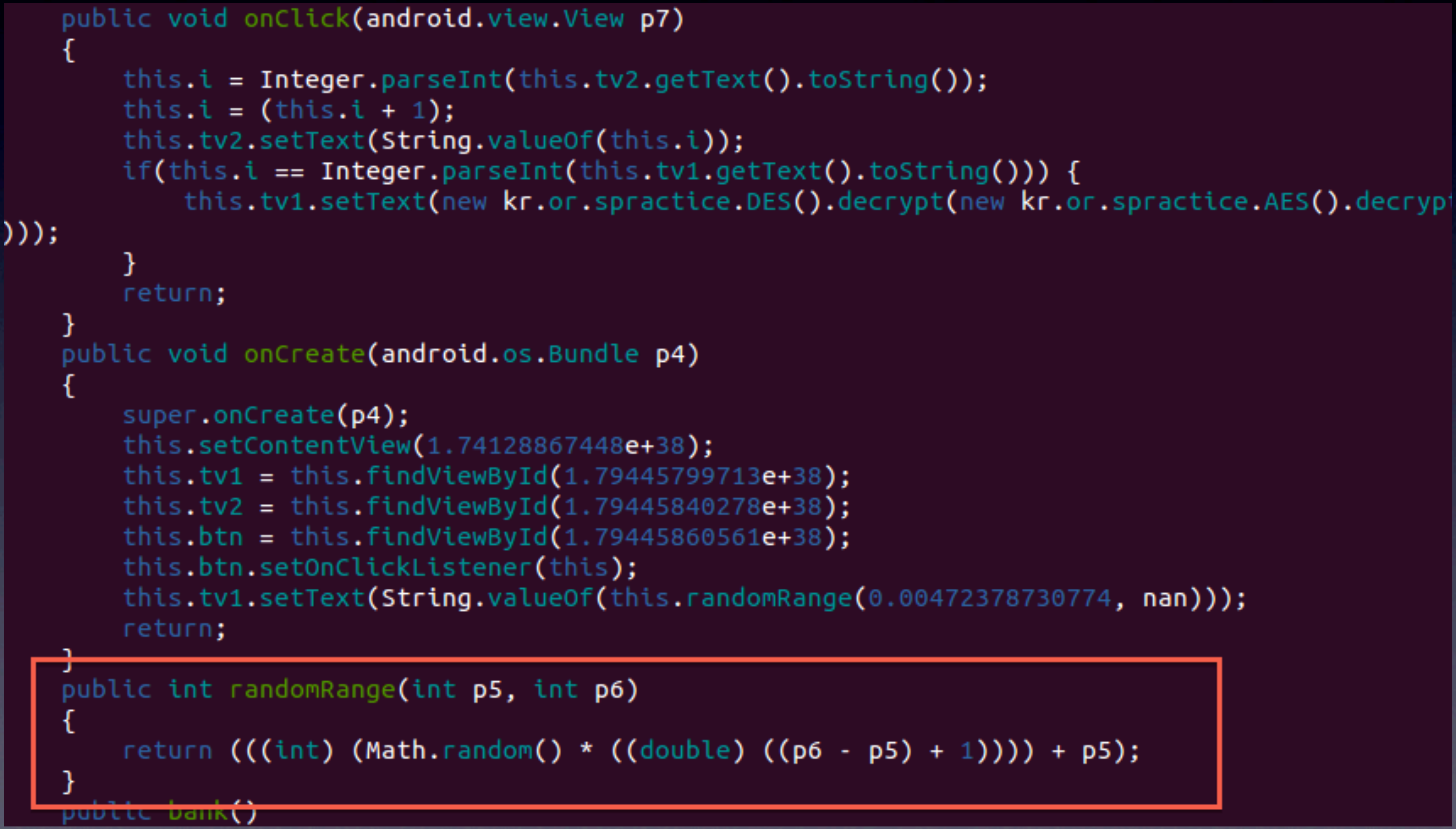
- APK리패키징 기법을 사용하지 않고 CydiaSubstrate Framework를 이용한 APK Hooking 구현.
- APK 직접수정없음.
- Android Java (Android Native는 다음에...)

Target APK

- sis.or.kr Mobile 3번문제 FindKey.apk
- APK파일을 수정하지 않음
- SmartPhone에 설치가능하도록 Sign만 했음.

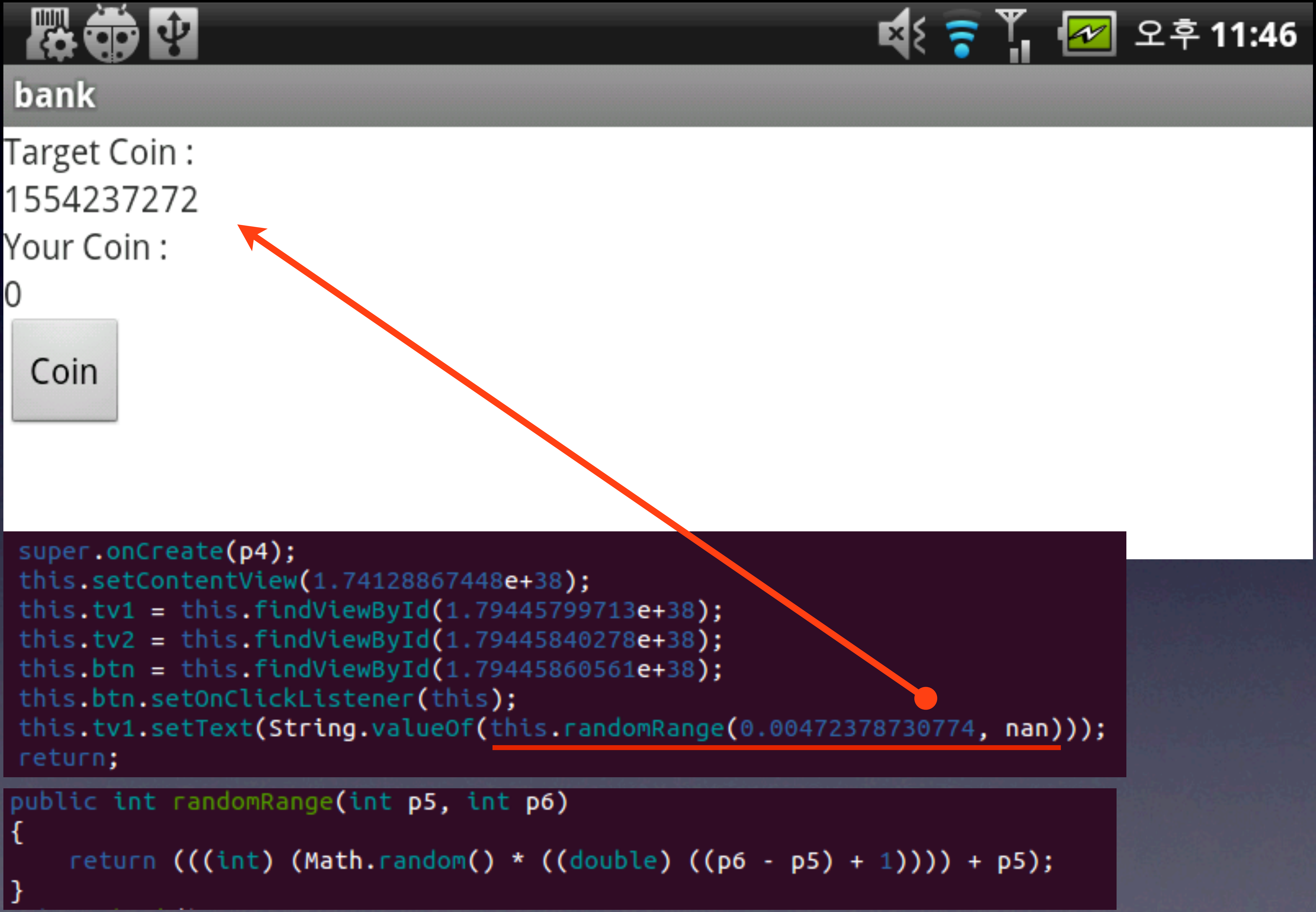
APK Hooking with CydiaSubstrate Framework

FindKey.apk bank Class



```
    public void onClick(android.view.View p7)
    {
        this.i = Integer.parseInt(this.tv2.getText().toString());
        this.i = (this.i + 1);
        this.tv2.setText(String.valueOf(this.i));
        if(this.i == Integer.parseInt(this.tv1.getText().toString())) {
            this.tv1.setText(new kr.or.spractice.DES().decrypt(new kr.or.spractice.AES().decrypt
)));
        }
        return;
    }
    public void onCreate(android.os.Bundle p4)
    {
        super.onCreate(p4);
        this.setContentView(1.74128867448e+38);
        this.tv1 = this.findViewById(1.79445799713e+38);
        this.tv2 = this.findViewById(1.79445840278e+38);
        this.btn = this.findViewById(1.79445860561e+38);
        this.btn.setOnClickListener(this);
        this.tv1.setText(String.valueOf(this.randomRange(0.00472378730774, nan)));
        return;
    }
    public int randomRange(int p5, int p6)
    {
        return (((int) (Math.random() * ((double) ((p6 - p5) + 1)))) + p5);
    }
    public bank()
```

APK Hooking with CydiaSubstrate Framework



bank

Target Coin :
1554237272
Your Coin :
0

```
super.onCreate(p4);
this.setContentView(1.74128867448e+38);
this.tv1 = this.findViewById(1.79445799713e+38);
this.tv2 = this.findViewById(1.79445840278e+38);
this.btn = this.findViewById(1.79445860561e+38);
this.btn.setOnClickListener(this);
this.tv1.setText(String.valueOf(this.randomRange(0.00472378730774, nan)));
return;
```

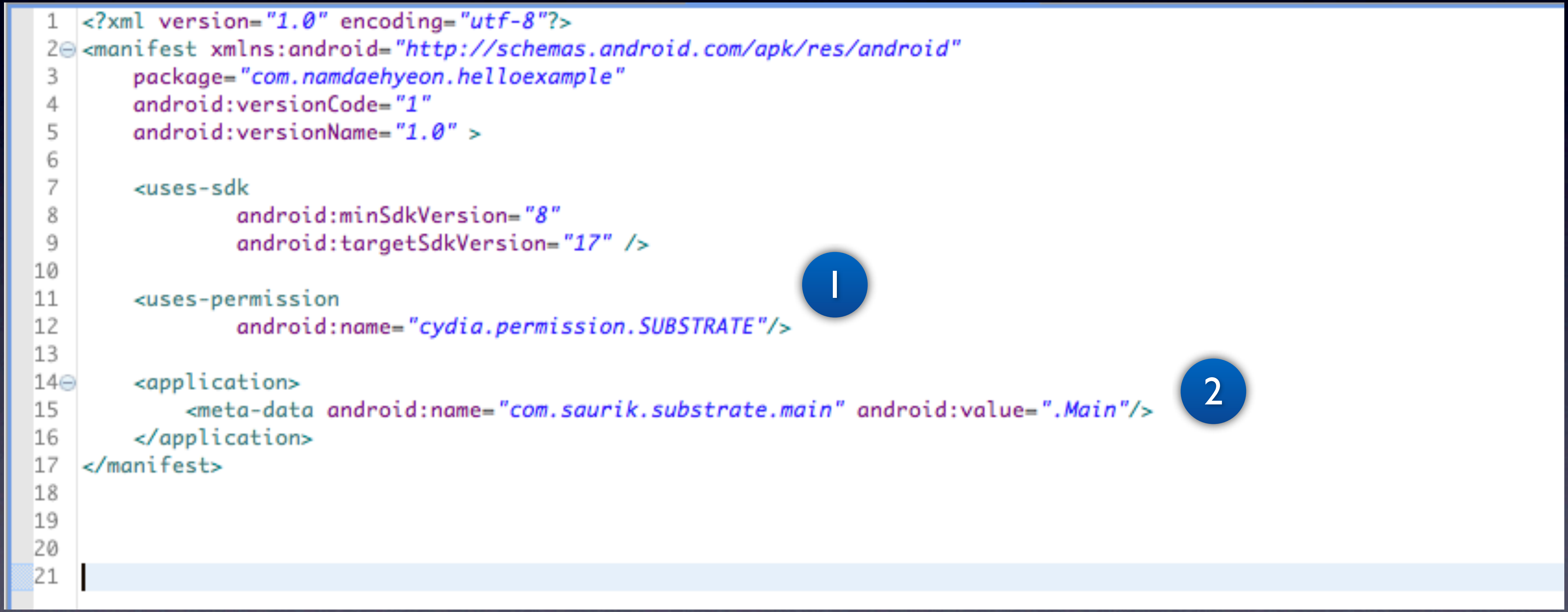
```
public int randomRange(int p5, int p6)
{
    return (((int) (Math.random() * ((double) ((p6 - p5) + 1)))) + p5);
}
```

Hooking Module 제작

- www.cydiasubstrate.com
- Code Injection (Android Java)
- substrate-api.jar 사용
- Eclipse + Android SDK 사용

APK Hooking with CydiaSubstrate Framework

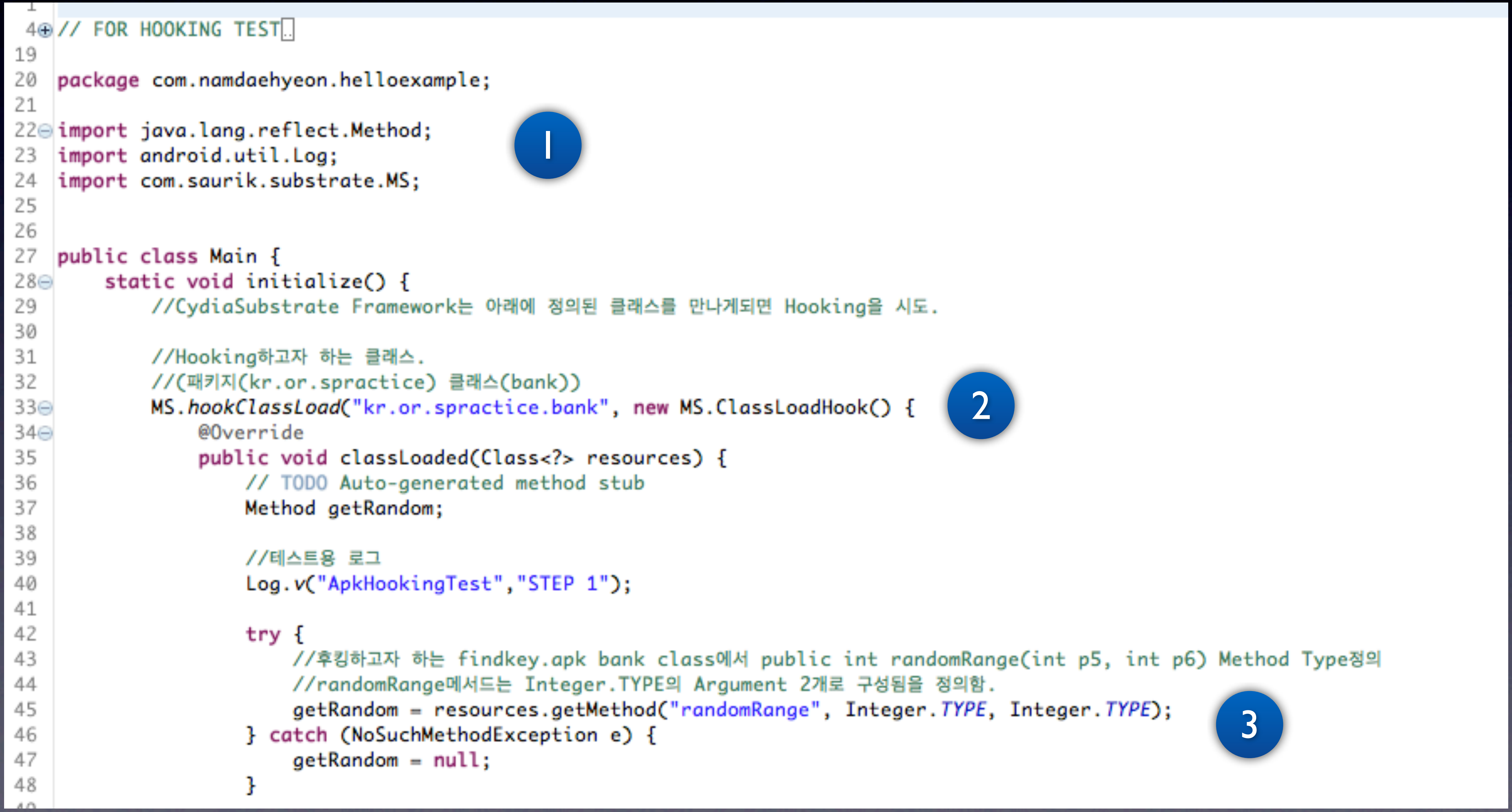
Sample Hooking Code



```xml
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.namdaehyeon.helloexample"
    android:versionCode="1"
    android:versionName="1.0" >

    <uses-sdk
            android:minSdkVersion="8"
            android:targetSdkVersion="17" />

    <uses-permission
            android:name="cydia.permission.SUBSTRATE"/>

    <application>
        <meta-data android:name="com.saurik.substrate.main" android:value=".Main"/>
    </application>
</manifest>



```

APK Hooking with CydiaSubstrate Framework

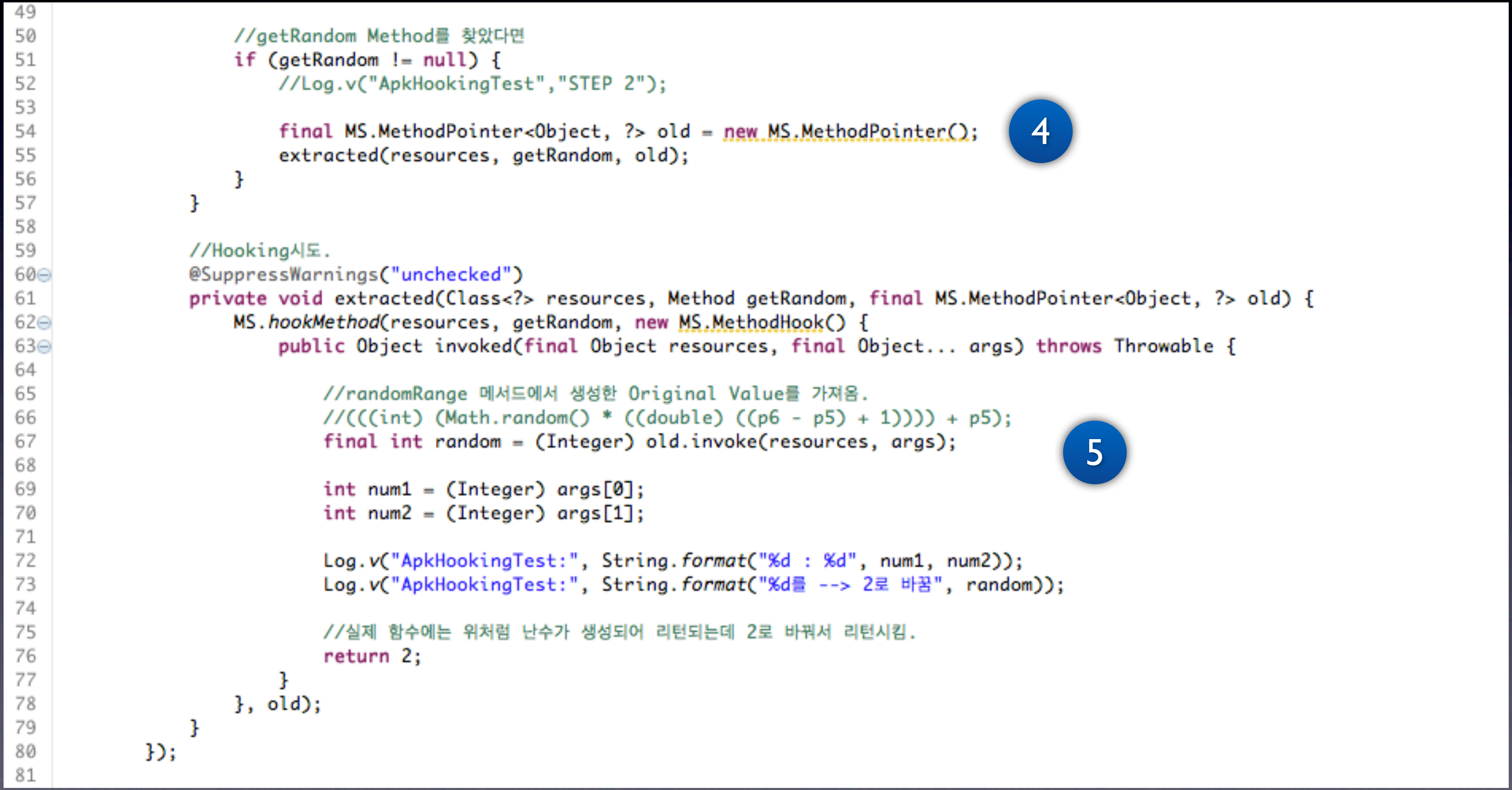
Sample Hooking Code



```
// FOR HOOKING TEST

package com.namdaehyeon.helloexample;

import java.lang.reflect.Method;
import android.util.Log;
import com.saurik.substrate.MS;


public class Main {
    static void initialize() {
        //CydiaSubstrate Framework는 아래에 정의된 클래스를 만나게되면 Hooking을 시도.

        //Hooking하고자 하는 클래스.
        //(패키지(kr.or.spractice) 클래스(bank))
        MS.hookClassLoad("kr.or.spractice.bank", new MS.ClassLoadHook() {
            @Override
            public void classLoaded(Class<?> resources) {
                // TODO Auto-generated method stub
                Method getRandom;

                //테스트용 로그
                Log.v("ApkHookingTest","STEP 1");

                try {
                    //후킹하고자 하는 findkey.apk bank class에서 public int randomRange(int p5, int p6) Method Type정의
                    //randomRange메서드는 Integer.TYPE의 Argument 2개로 구성됨을 정의함.
                    getRandom = resources.getMethod("randomRange", Integer.TYPE, Integer.TYPE);
                } catch (NoSuchMethodException e) {
                    getRandom = null;
                }
```

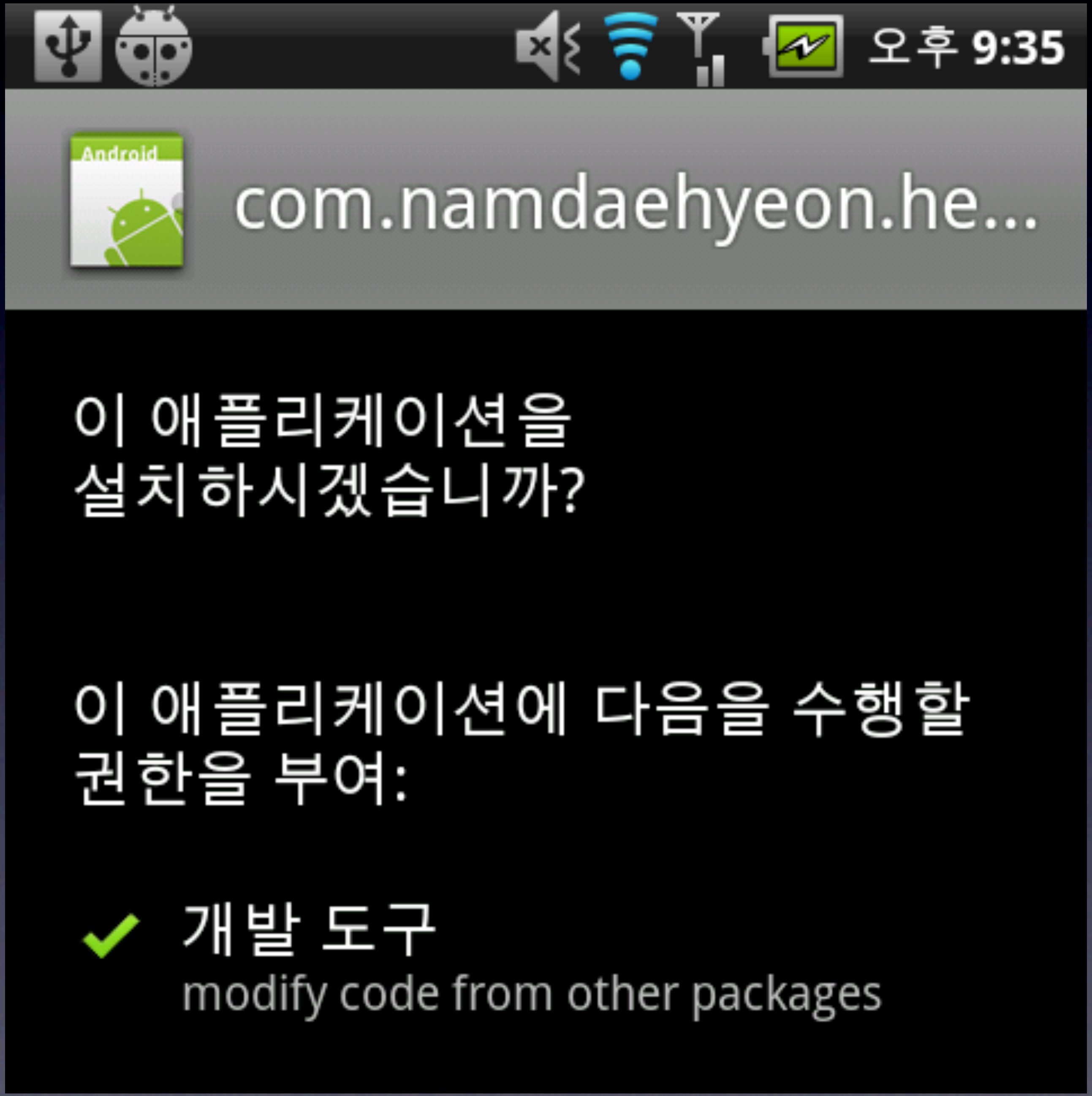
APK Hooking with CydiaSubstrate Framework

Sample Hooking Code



```
                //getRandom Method를 찾았다면
                if (getRandom != null) {
                    //Log.v("ApkHookingTest","STEP 2");

                    final MS.MethodPointer<Object, ?> old = new MS.MethodPointer();
                    extracted(resources, getRandom, old);
                }
            }

            //Hooking시도.
            @SuppressWarnings("unchecked")
            private void extracted(Class<?> resources, Method getRandom, final MS.MethodPointer<Object, ?> old) {
                MS.hookMethod(resources, getRandom, new MS.MethodHook() {
                    public Object invoked(final Object resources, final Object... args) throws Throwable {

                        //randomRange 메서드에서 생성한 Original Value를 가져옴.
                        //(((int) (Math.random() * ((double) ((p6 - p5) + 1)))) + p5);
                        final int random = (Integer) old.invoke(resources, args);

                        int num1 = (Integer) args[0];
                        int num2 = (Integer) args[1];

                        Log.v("ApkHookingTest:", String.format("%d : %d", num1, num2));
                        Log.v("ApkHookingTest:", String.format("%d를 --> 2로 바꿈", random));

                        //실제 함수에는 위처럼 난수가 생성되어 리턴되는데 2로 바꿔서 리턴시킴.
                        return 2;
                    }
                }, old);
            }
        });
```

APK Hooking with CydiaSubstrate Framework



오후 9:35

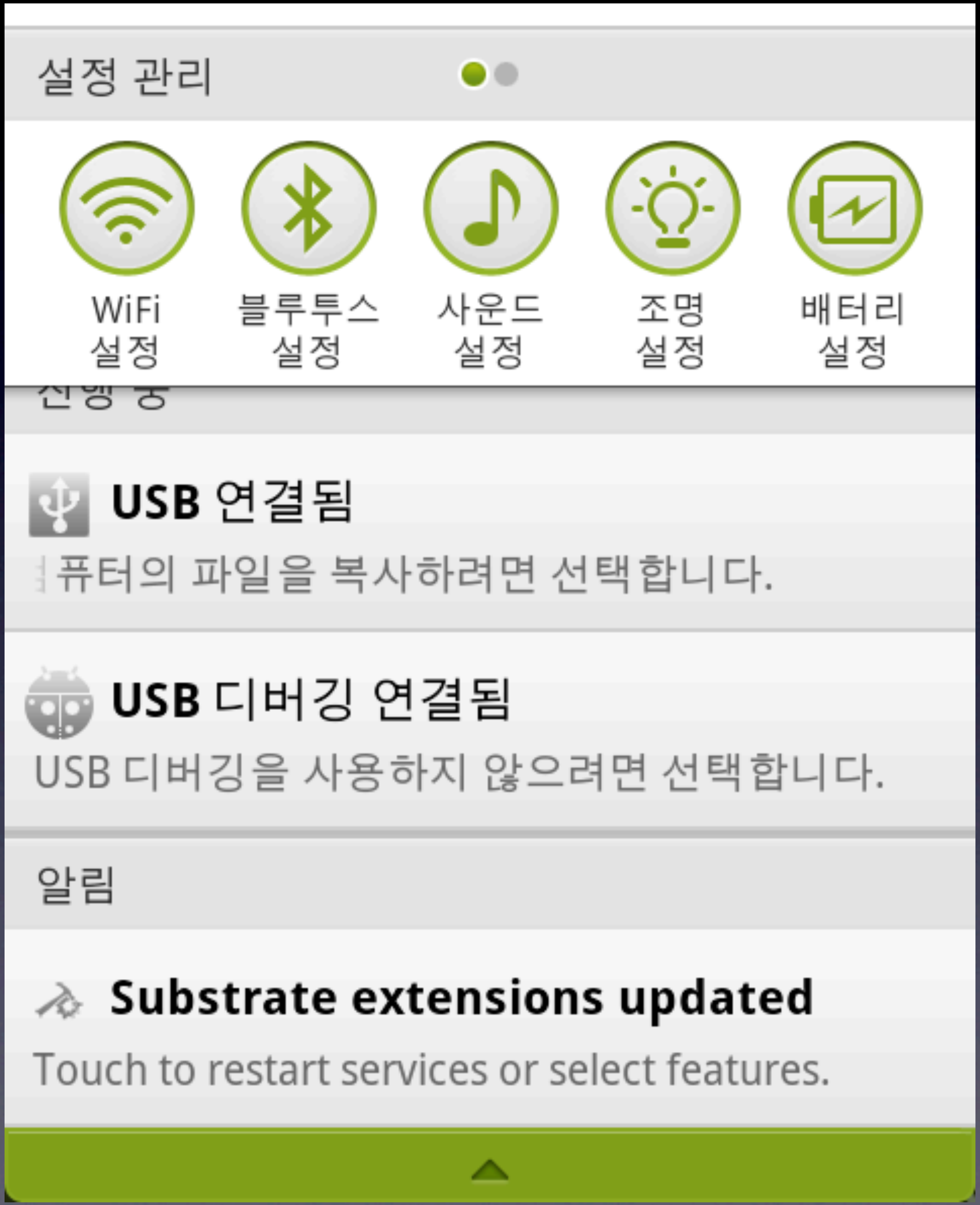
com.namdaehyeon.he...

이 애플리케이션을
설치하시겠습니까?

이 애플리케이션에 다음을 수행할
권한을 부여:

✓ 개발 도구
modify code from other packages

APK Hooking with CydiaSubstrate Framework



설정 관리

진행 중

USB 연결됨

퓨터의 파일을 복사하려면 선택합니다.

USB 디버깅 연결됨

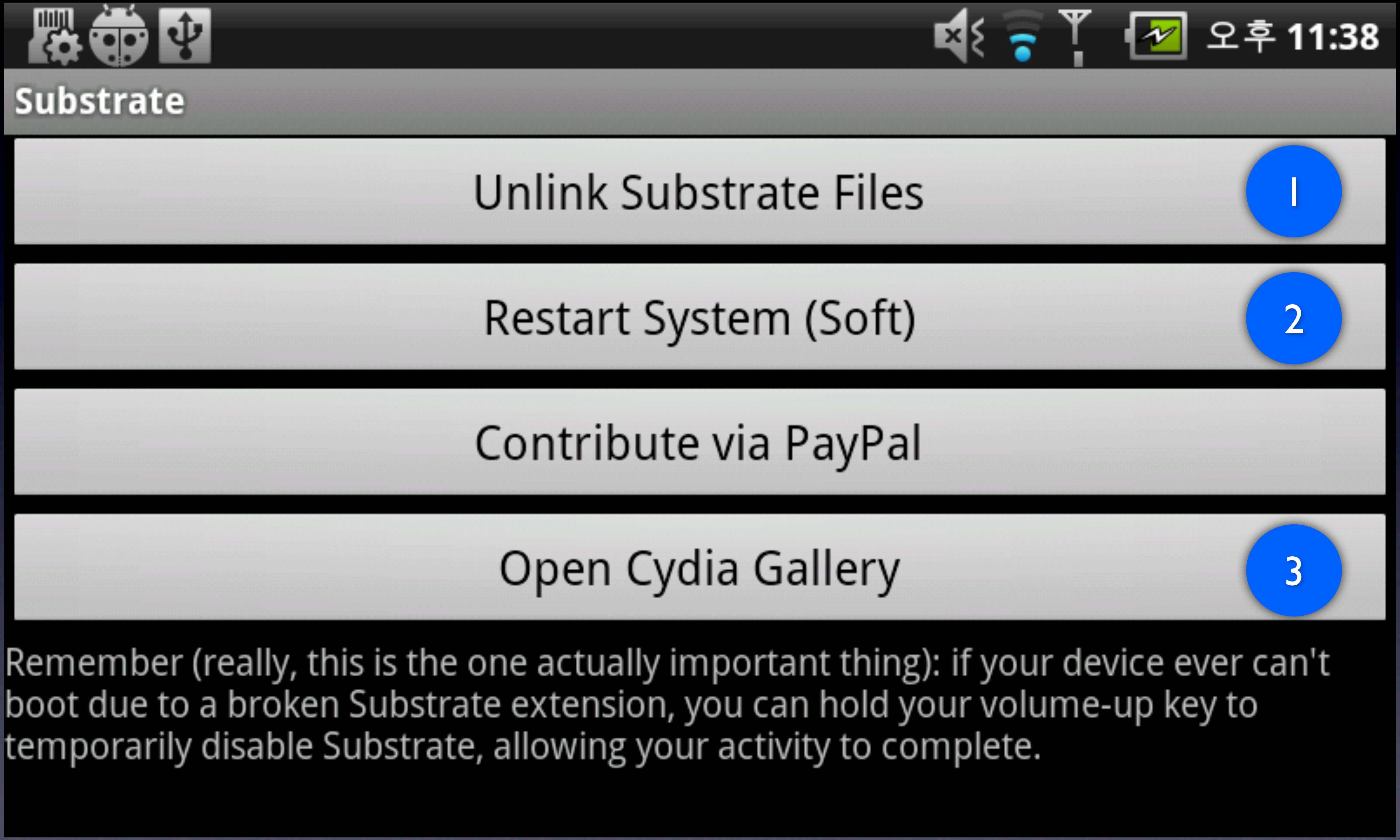
USB 디버깅을 사용하지 않으려면 선택합니다.

알림

Substrate extensions updated

Touch to restart services or select features.

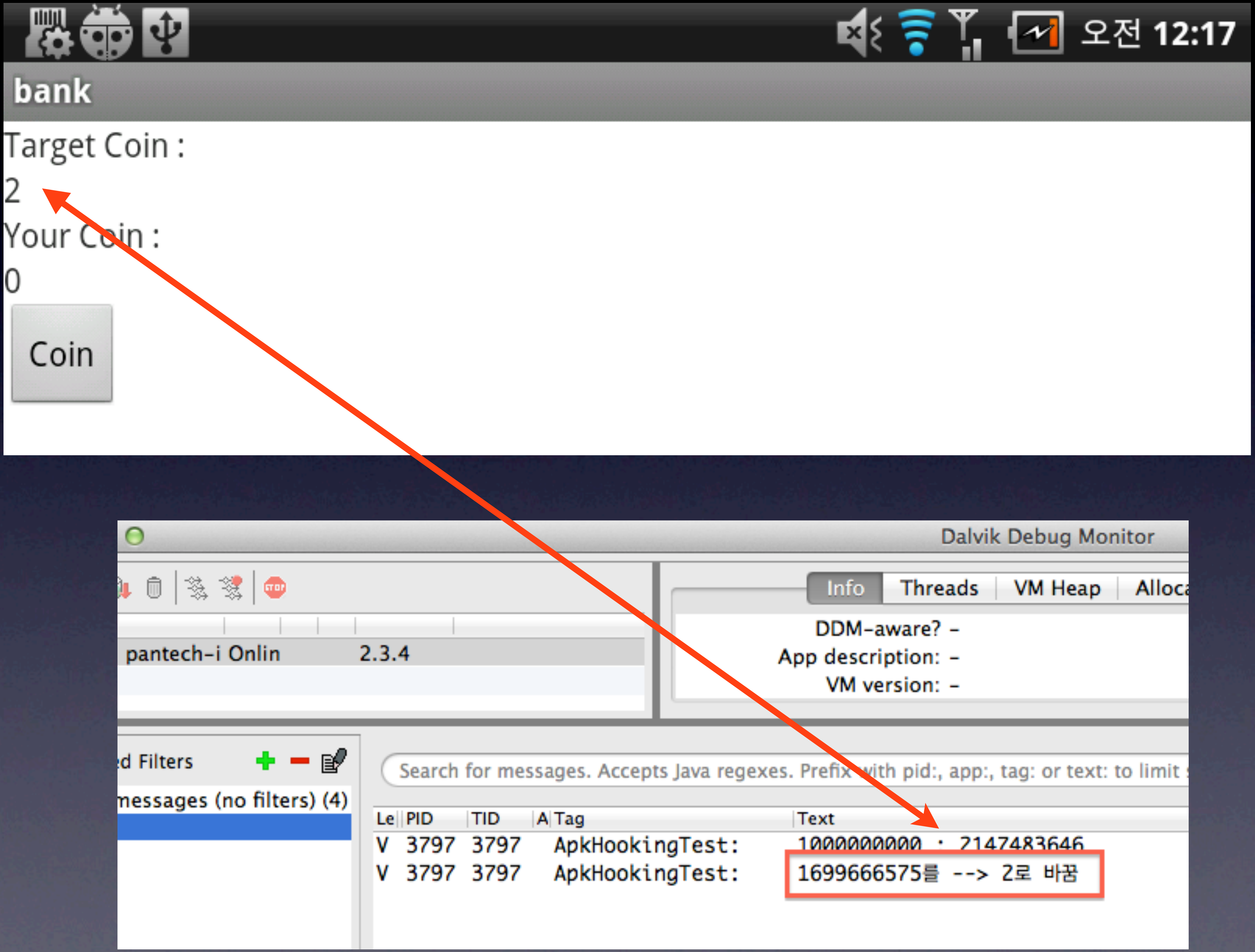
APK Hooking with CydiaSubstrate Framework



Remember (really, this is the one actually important thing): if your device ever can't boot due to a broken Substrate extension, you can hold your volume-up key to temporarily disable Substrate, allowing your activity to complete.

1: Hooking Module 활성/비활성
2: 설치한 Hooking Module적용을 위한 SmartPhone Reboot

APK Hooking with CydiaSubstrate Framework



Target Coin :
2
Your Coin :
0

DDM-aware? -
App description: -
VM version: -

Search for messages. Accepts Java regexes. Prefix with pid:, app:, tag: or text: to limit

```
Le PID   TID   A Tag               Text
V  3797  3797    ApkHookingTest:   1000000000 : 2147483646
V  3797  3797    ApkHookingTest:   1699666575를 --> 2로 바꿈
```

END

2013.5.19

namdaehyeon [nam_daehyeon@naver.com]