



Android AIDS In CSharp:

Automatic Intelligence De-advertisement Scheme

Hello!

aaaddress1(ADR)

1. Reverse Engineering Skill
 - a. Windows
 - b. Android
2. TDoHacker Core Member
3. Hack Bot
 - a. CrackShield / MapleHack
 - b. Tower Of Savior
 - c. FaceBook
4. CSharp,C/C++,Assembly x86
Python,Smali,Pascal,VB.NET





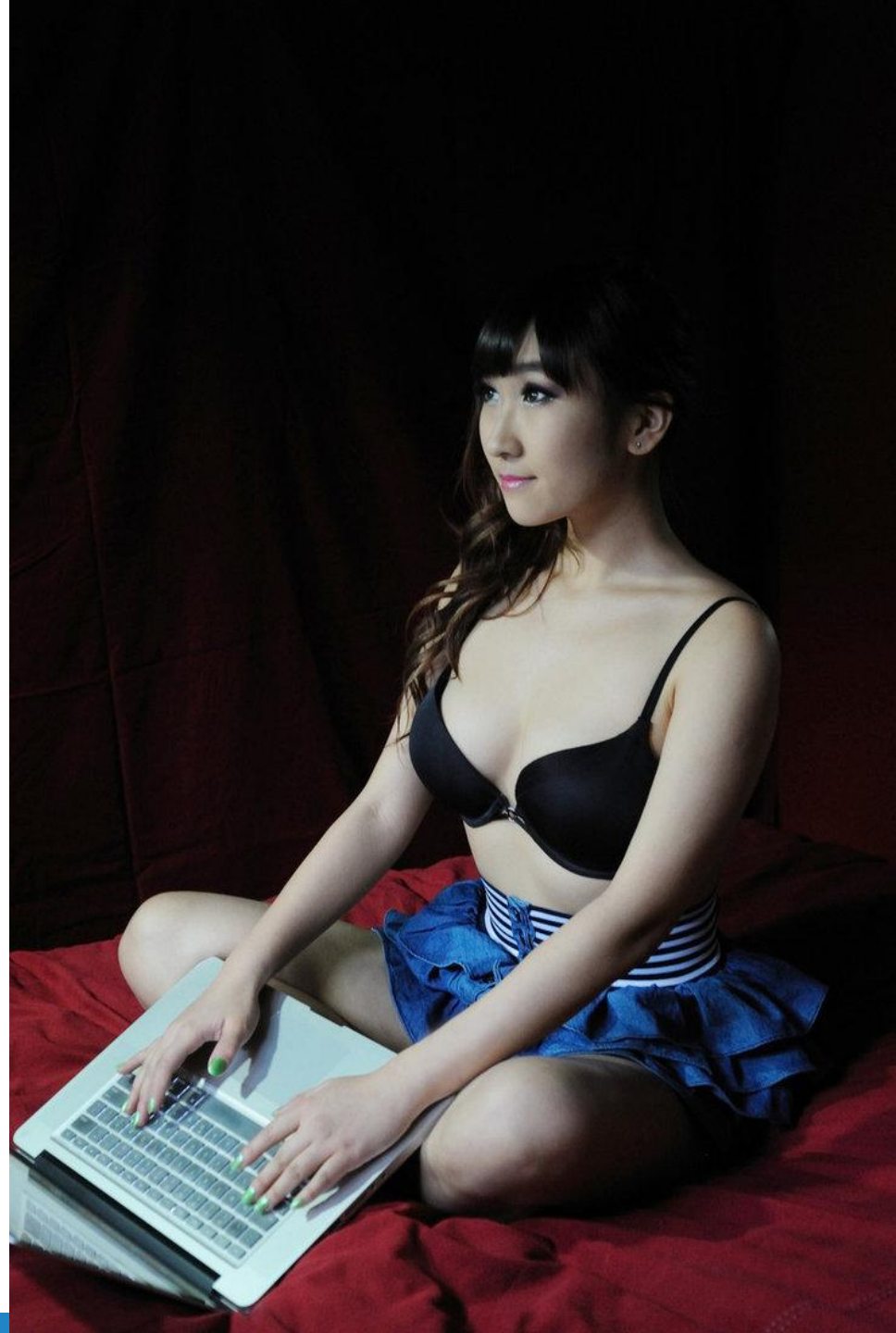
Outline

- Why Do We Need AIDS?
- How Ads Were Displayed?
- How Android Works.
- Android Basic Cracking.
- Live Demo Of Patching Ads In APK.
- Ads In Game Engine: Unity.
- ProGuard Obfuscation.
- How To Build This Tool In CSharp.
- Live Demo.



Why Do We Need AIDS?

To Surf The
Net.





To Surf The Net







搜尋人、地點和事物



聖豪

首頁



結果還是GG，上面那指令還真的有想過（抹臉）

讚 · 6月25日 23:34

查看更多回覆



尤理衡 嘿嘿

讚 · 回覆 · 23小時



留言.....



韋倪豪和柯炯胜都分享了 7Lions 的影片。



1,086,988 次觀看

7Lions

When you really gotta get away from the photogs.!

參考翻譯

贊助

刊登廣告



Ur ANDROID App Ranks 1st?

www.mobileaction.co

Get your ANDROID App Ranked 1st with our FREE optimization tool!



Capcom卡普空

一起來狩獵喔！

G5大型改版 全面進化 全新古龍種魔物「雅翁龍」勢如破竹來襲！一起來狩獵吧！

中文(台灣) · 隱私政策 · 使用條款 · Cookies · 廣告 · 廣告選擇 · 更多

Facebook © 2015





您的 Mac 运行迟缓?

清理 Mac 上的系统垃圾, 让其运行更快! [立即下载](#)

Google 提供的广告



Nicki Minaj - Anaconda



NickiMinajAtVEVO

 訂閱 8,786,358

477,063,287

 新增至  分享  更多

 1,983,713  972,653

您的 Mac 运行迟缓?
清理 Mac 上的系统垃圾, 让其运行更快!



MacKeeper

拖至 此处
下载

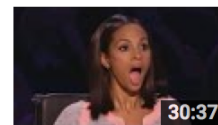


应用程序

立即下载

即将播放

自动播放 

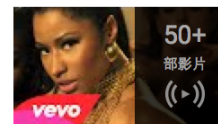


Top 10 Best magicians Got talent

由Kino Trailers建立

观看次数: 5,888,496

30:37



合辑 - Nicki Minaj - Anaconda

上传者: YouTube

50+
部影片
(>)



Nicki Minaj - Starships (Clean)

由NickiMinajAtVEVO建立

观看次数: 38,465,559

4:22



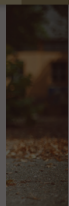
天下雜誌部落格

連結人與人之間的新觀點

(專欄反映作者意見，不代表天下立場)

最新文章

科技部落格



以從孩



藍白拖／人生

編輯推薦好文



陳仁豪／婚姻也是有交易成本的

身體部位

VoiceTube

原來Umbilicus是肚臍！

教你腋下、鬢角等奇怪部位的英文

VoiceTube／別再用中文邏輯學英文，學好英文前你需要一顆「英文腦」！

詹長霖／累死你的不是工作，而是工作方法

蔡淇華／我們或許不是天使，「選擇」卻能造就我們長出光環

老貓／出暢銷

How To Remove Ads On WebBrowser: Clearly

Chrome 線上應用程式商店

搜尋店內商品

應用程式

擴充功能

主題

類型

☐ Chrome 應用

☐ 網站

類別

全部

功能

☐ 可在離線狀態下使用

☐ Google 製作

☐ 免費

☐ 適用於 Android

☐ 支援 Google Play 服務

評分

☐ ★★★★★

Clearly

來源網站: evernote.com

★★★★★ (3243) 實用工具 1,127,720 位使用者

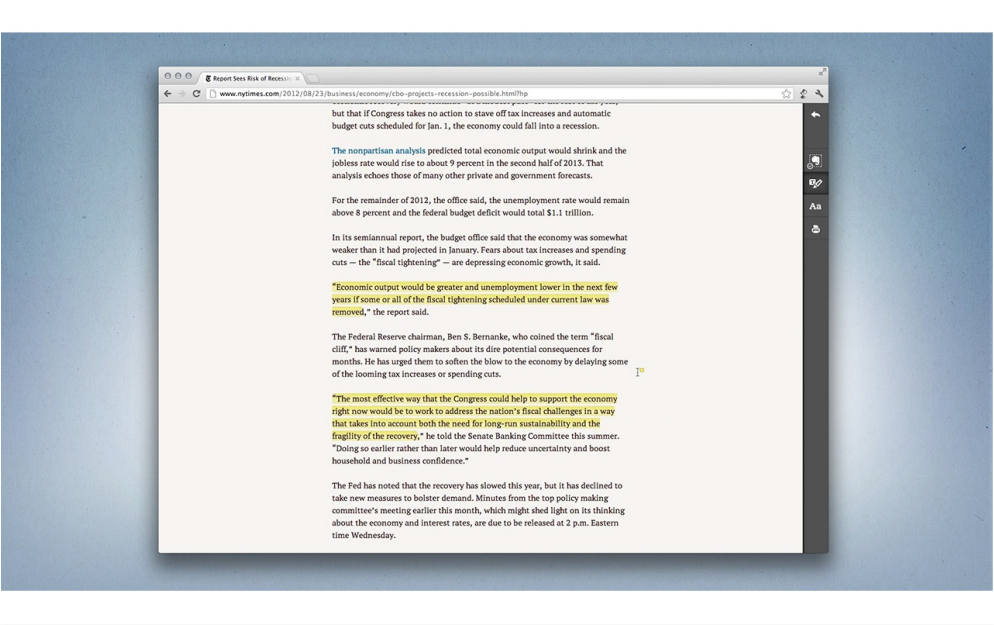
總覽

評論

支援

相關項目

8+1 6,622



加到 CHROME

Clearly 可使部落格發佈、文章與網頁乾淨而容易閱讀。請將其儲存至 Evernote 以便於任何位置閱讀。

只要按一下滑鼠鍵，Clearly 便可使部落格發佈與文章乾淨而容易閱讀。Clearly 可使您在線上閱讀的體驗中免除遭遇分心的情況，甚至可以讓您在單一、無縫的視圖中瀏覽多頁文章。

將 Clearly 連接至 Evernote，可透過您所使用的每一部電腦、手機與平板電腦進行裁剪與同步。

自訂
從三個視圖中選擇或建立您自己的視圖。可自訂的鍵盤捷徑可以讓您快速啟動 Clearly，並直接將文章裁剪到 Evernote 中。

網址

網站

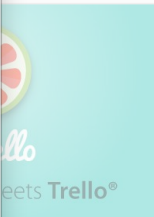
檢舉濫用情形

版本: 10.6.1.8
更新日期: 2015年6月11日
大小: 1.35MB
語言: [查看全部 22 種語言](#)

aaaddress1@gmail.com



查看全部



免費

How To Remove Ads On WebBrowser: AdBlock

Facebook 的颜色变化

來源網站: partido.me

[加到 CHROME](#)
 社交網路
 ★★★★★ (1494)
 ⚡
[加到 CHROME](#)
 搜尋和瀏覽工具
 ★★★★★ (1018)
 ⚡
[加到 CHROME](#)
 實用工具
 ★★★★★ (38871)
 ➔
[加到 CHROME](#)
 實用工具
 ★★★★★ (77726)
 ➔
[加到 CHROME](#)
 協助工具
 ★★★★★ (7892)

功能

- ☐ 可在離線狀態下使用
- ☐ Google 製作
- ☐ 免費
- ☐ 適用於 Android
- ☐ 支援 Google+

AdBlock

來源網站: getadblock.com

★★★★★ (139046) [實用工具](#) 10,000,000+ 位使用者

總覽
評論
支援
相關項目

g+
上萬

AdBlock. The #1 ad blocker with over 200 million downloads. Blocks YouTube, Facebook and ALL ads by default (unlike Adblock Plus).

The original AdBlock for Chrome. Block all advertisements on all web pages, even Facebook, Youtube, and Hulu.

It works automatically: just click "Add to Chrome," then visit your favorite website and see the ads disappear!

You can also get AdBlock for Safari, Opera, and Firefox from getadblock.com.

PS: Like it? Please follow AdBlock on G+ at [Google+](#)

[網站](#)

[檢舉濫用情形](#)

版本: 2.35
 更新日期: 2015年6月10日
 大小: 864KB
 語言: [查看全部 34 種語言](#)

**TOYOTA**
Let's Go Places

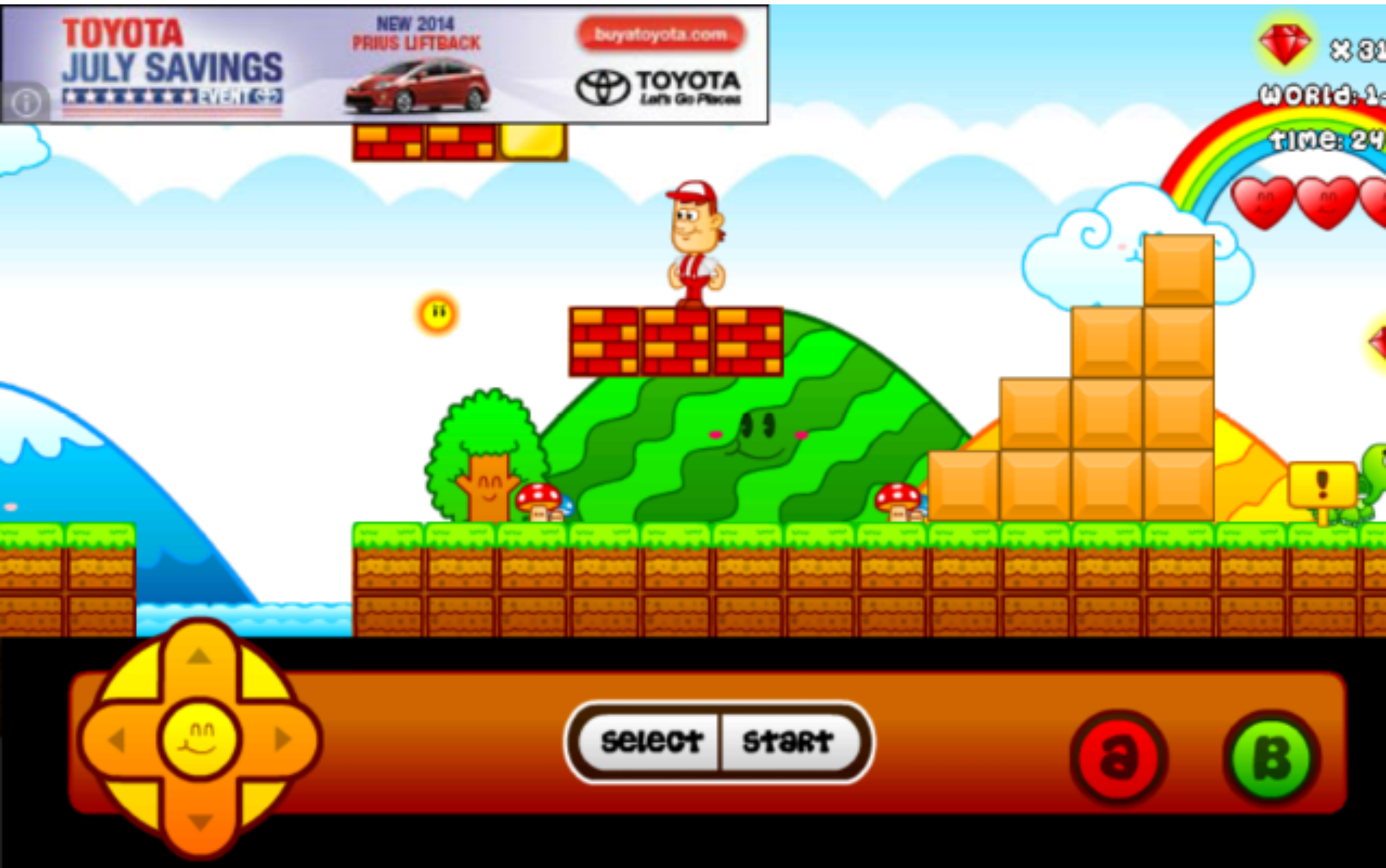
NEW 2014
PRIUS LIFTBACK



TOYOTA
JULY SAVINGS

*****REVENUE**

buyatoyota.com



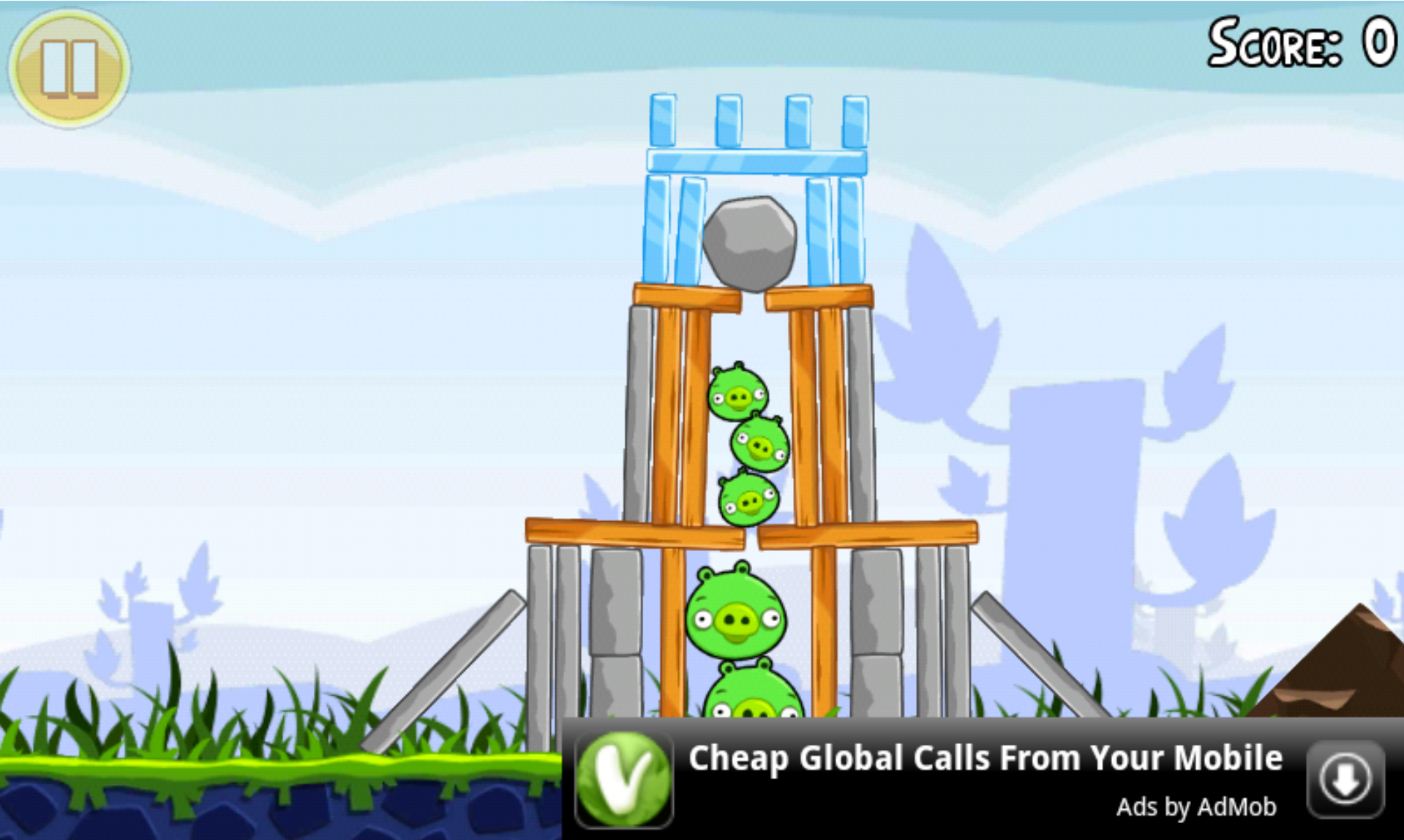


SAVING YELLO

Save Yello from his
out-of-bowl terror!

FREE
download!

SCORE: 0





But...

How To Remove Ads On Android?

Remove Ads On Android: AdAway

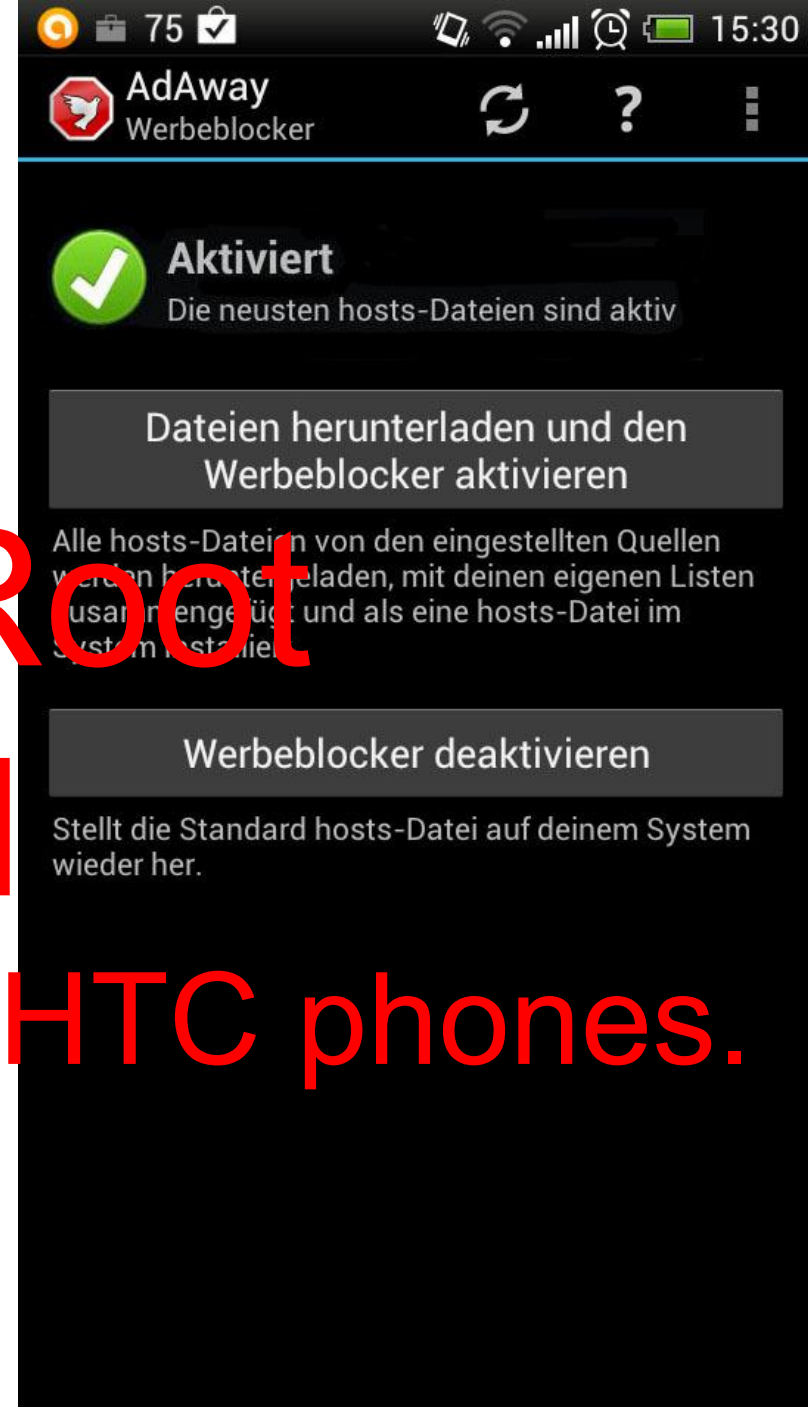
AdAway lets you select your own sources of hosts files
You can add exceptions to your Whitelist
if an app is not working when specific hosts are blocked

You can define extra hostnames in your own Blacklist. You
can add your own (hostname, IP-pairs) in the Redirection
List

Requirements

Android version: 2.1+ ROOT required Read/Write access to
system-Partition Problems can occur on some HTC devices
when system-Partition is not writable!

**Need Root
And
might not work on HTC phones.**



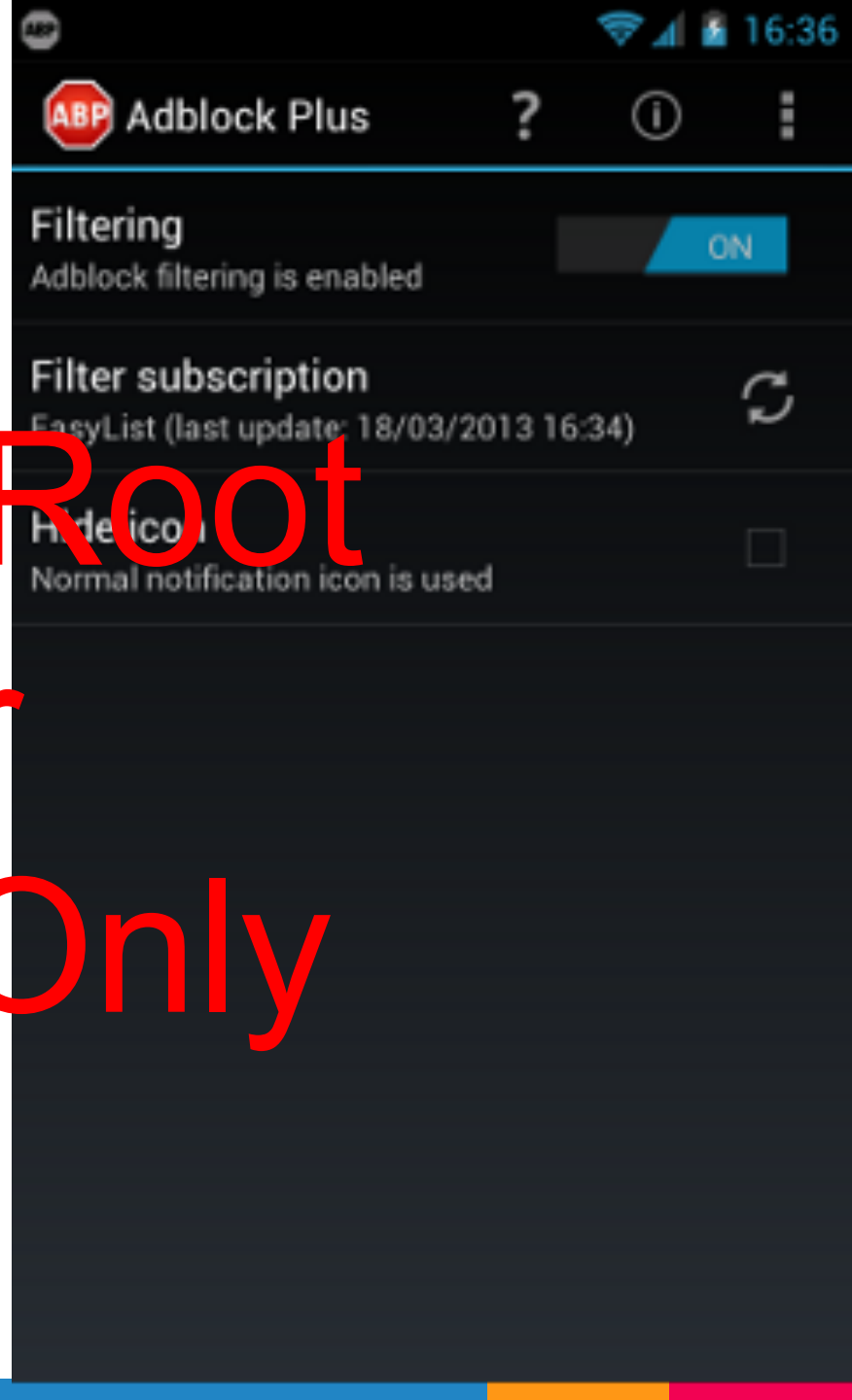
Remove Ads On Android: Adblock

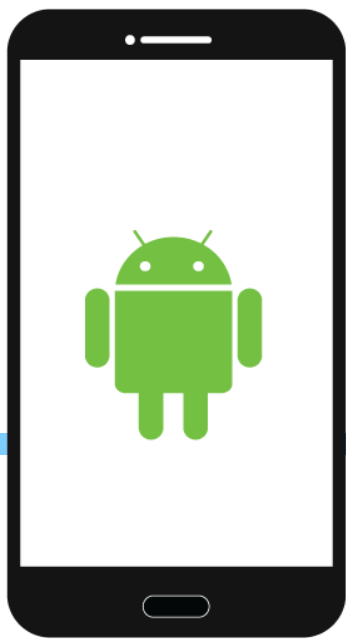
若裝置 已取得 root 權限,
則 Adblock Plus 會自動過濾所有網路流量。

On non-rooted devices running Android 4.1.2, 4.2.1 and higher, Adblock Plus will filter all WiFi traffic, but it needs to be configured as a proxy server manually. Detailed instructions are provided by Adblock Plus for not experienced users.

對於未取得 root 權限及執行 Android 3.1 以上版本的裝置, Adblock Plus 僅會過濾透過 WiFi 連線的網路流量。對於未取得 root 權限及執行 Android 3.0 以下版本的裝置, 則需要手動將 Adblock Plus 設定為一個代理伺服器。部分裝置不支援代理伺服器設定, Adblock Plus 自然也就無法在這些裝置上運作。

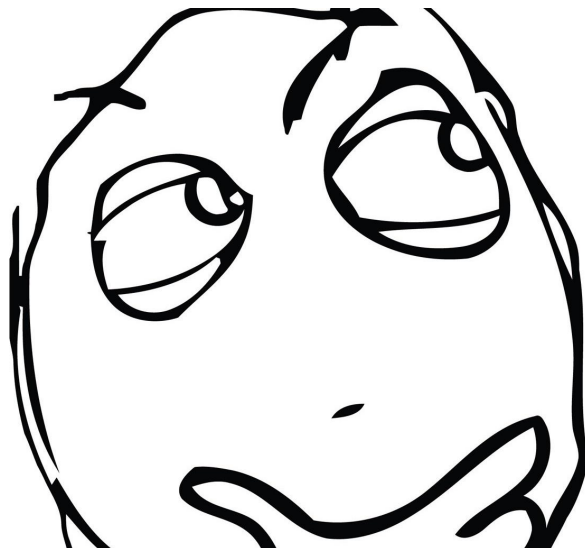
Need Root
Or
WiFi Only





3G / 4G

*If I Have An Android Phone
But ... I Don't Have Root...*





Mitsun Chieh 沒有女朋友就new一個出來，想要什麼屬性跟功能隨你！



12月12日 14:07 · 收回讚 · 13



Could We Remove Those Ads On Android?

<  安全性

裝置管理

裝置管理員

檢視或停用裝置管理員

未知的來源

允許從來源安裝的應用程式，而非 Play Store



認證儲存空間

受信任的認證

顯示信任的 CA 憑證

If we can...

APK

Patched Ads
APK





How Ads Were Displayed



Android M Developer Preview

Get your apps ready for the next version of Android. Test on Nexus 5, 6, 9, and Player.

> Get started



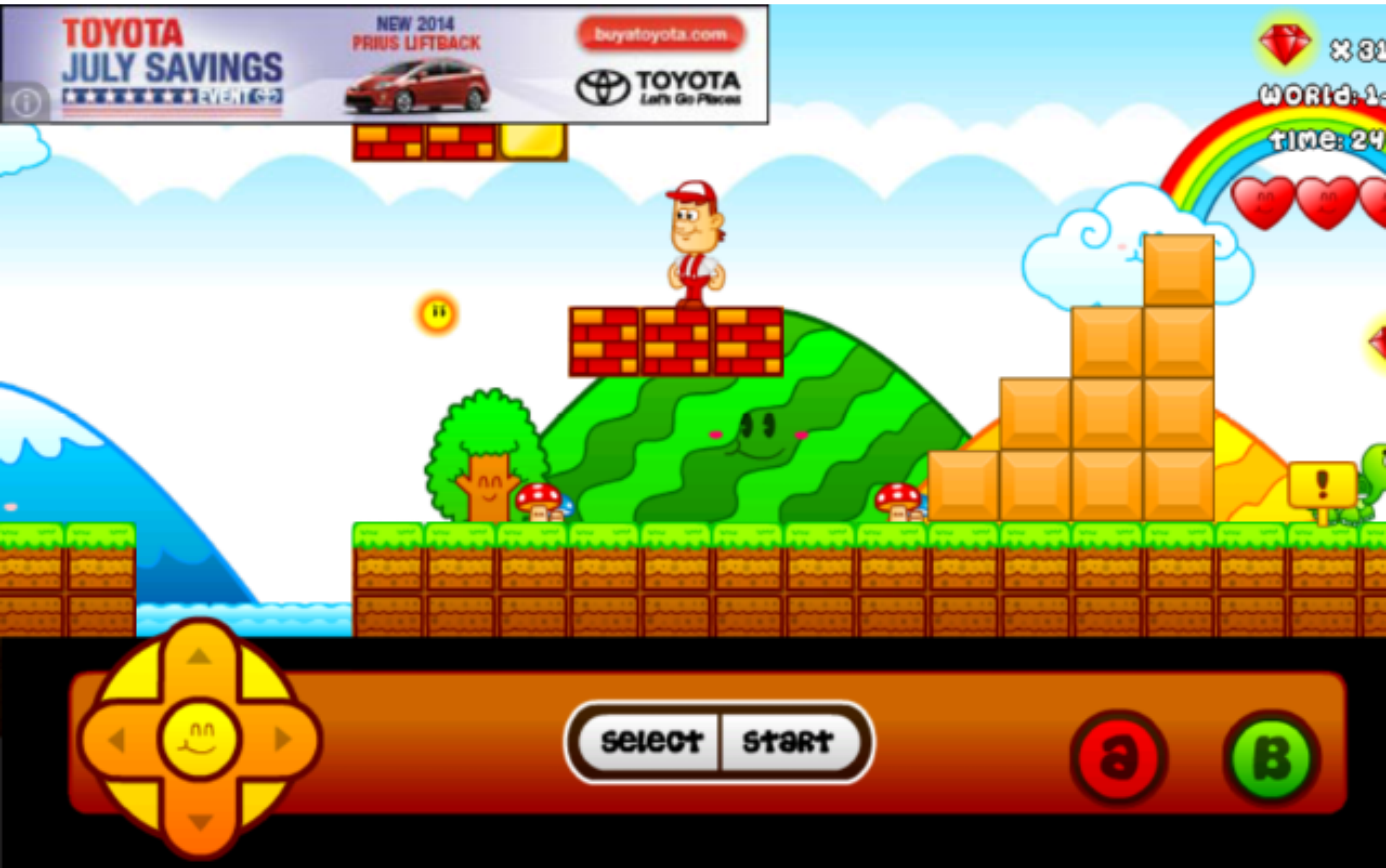
TOYOTA
JULY SAVINGS
*****REVENUE*****

NEW 2014
PRIUS LIFTBACK

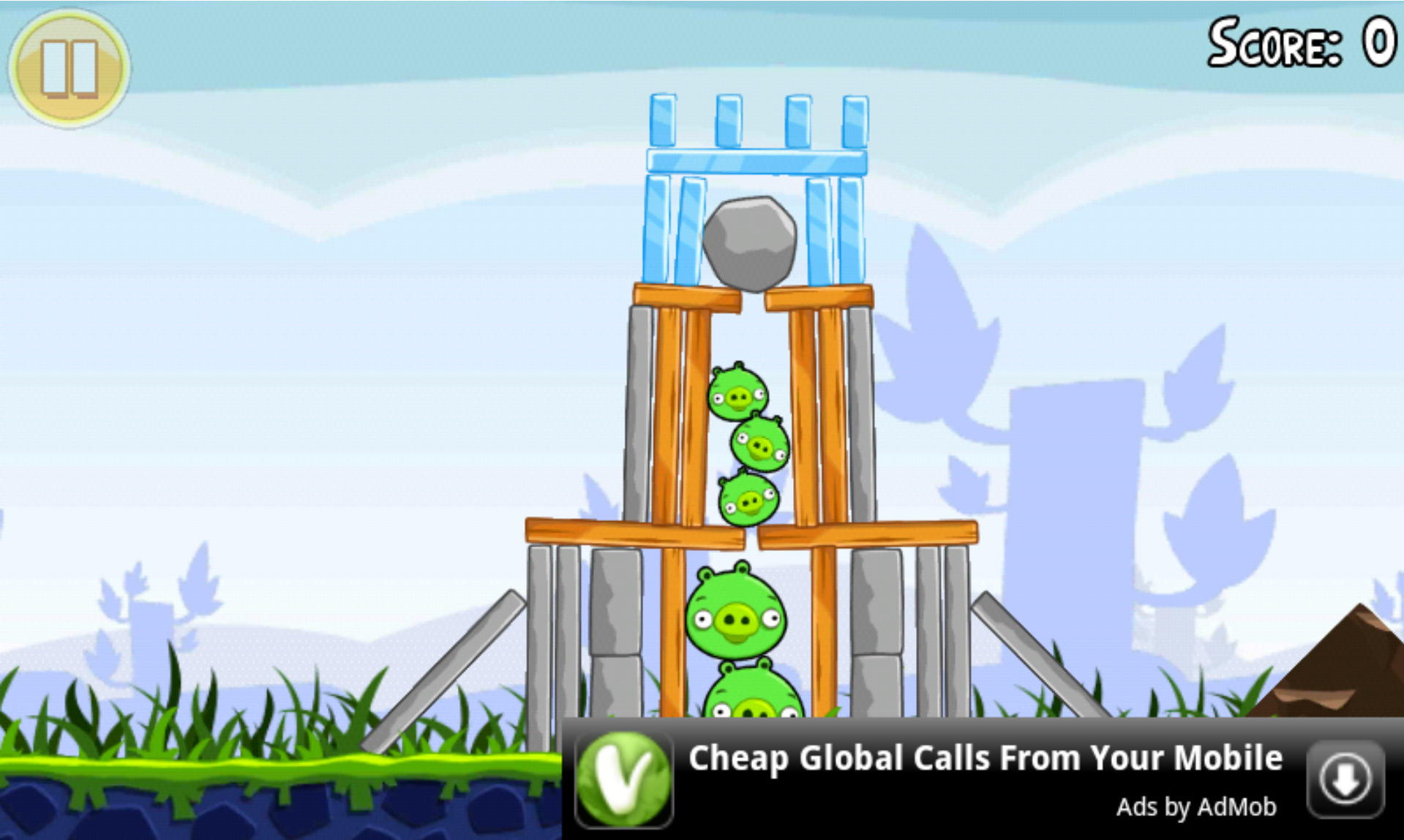


buyatoyota.com

 **TOYOTA**
Let's Go Places



SCORE: 0



AdView



public final class **AdView** extends [ViewGroup](#)

[java.lang.Object](#)

↳ [android.view.View](#)

↳ [android.view.ViewGroup](#)

↳ [com.google.android.gms.ads.AdView](#)

The [View](#) to display banner ads. The ad size and ad unit ID must be set prior to calling [loadAd\(AdRequest\)](#).

Publishers using DoubleClick for Publishers or Search Ads for Apps should use [PublisherAdView](#) or [SearchAdView](#), respectively.

AdView Type Ads

// Create a banner ad. The ad size and ad unit ID must be set before calling loadAd.

```
mAdView = new AdView(this);  
mAdView.setAdSize(AdSize.SMART_BANNER);  
mAdView.setAdUnitId("myAdUnitId");
```

// Create an ad request.

```
AdRequest.Builder adRequestBuilder = new AdRequest.Builder();
```

// Add the AdView to the view hierarchy.

```
layout.addView(mAdView);
```

// Start loading the ad.

```
mAdView.loadAd(adRequestBuilder.build());
```



SAVING YELLO

Save Yello from his
out-of-bowl terror!

FREE
download!

InterstitialAd



public final class **InterstitialAd** extends [Object](#)

[java.lang.Object](#)



com.google.android.gms.ads.InterstitialAd

Full-screen interstitial ads. The ad unit ID must be set prior to calling [loadAd\(AdRequest\)](#) .

Publishers using DoubleClick for Publishers should use [PublisherInterstitialAd](#) .

InterstitialAd Type Ads

```
//If the interstitial is finished loading,  
//the user will view the interstitial before proceeding.  
mInterstitialAd = new InterstitialAd(this);  
mInterstitialAd.setAdUnitId("myAdUnitId");  
  
// Create an ad request.  
AdRequest.Builder adRequestBuilder = new AdRequest.Builder();  
  
// Optionally populate the ad request builder.adRequestBuilder.addTestDevice  
(AdRequest.DEVICE_ID_EMULATOR);  
mInterstitialAd.loadAd(adRequestBuilder.build());
```



new
ADView



setAdSize



loadAd

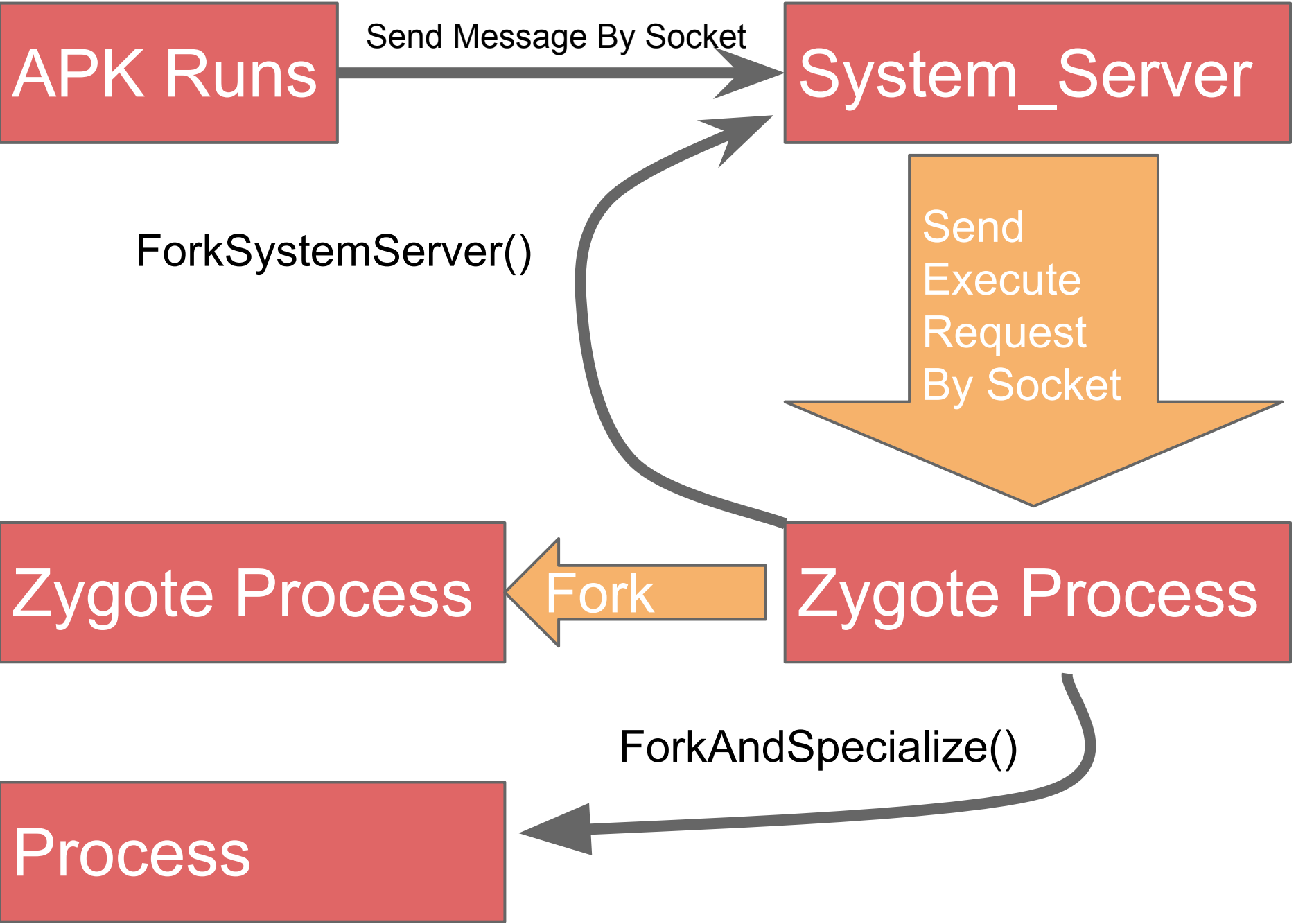
new
InterstitialAd

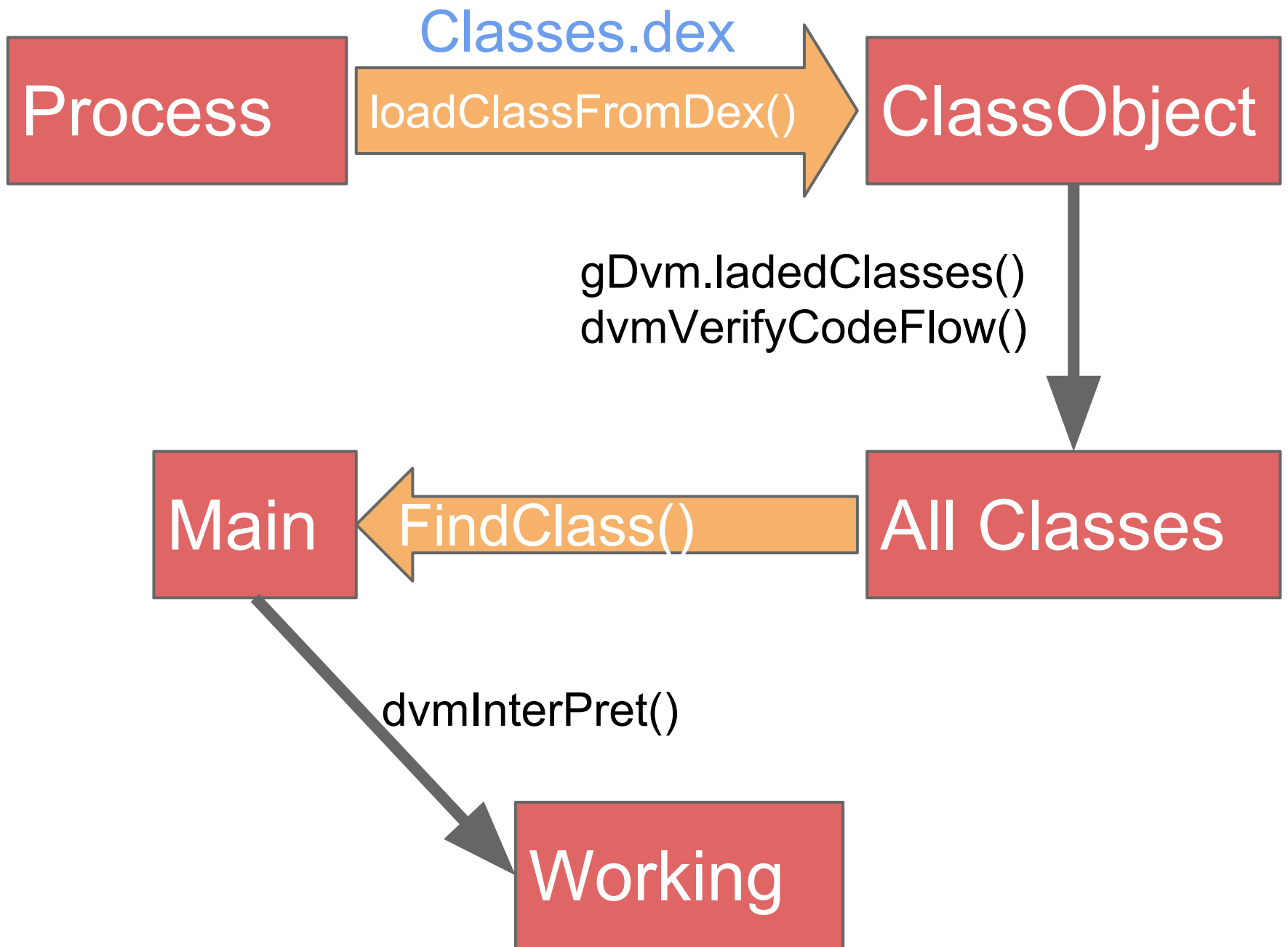


loadAd



How Android Works





How APP Works On Android

1. Process Created By Zygote Process
2. APP Code Load By `loadClassFromDex()`
To Load `Classes.dex` From APK
3. Get All Classes By `gDvm.ladedClasses()`
4. APK Base On Class Unit



Android Basic Cracking



We know that APK runs on Android this way

APK
Package

Check Sign
& Extract

Classes.dex



We know that APK runs on Android this way

Classes.dex

DexFile.loadDex()

Dalvik
VM



How We Do Code Review of Classes.dex?



smali

An assembler/disassembler for Android's dex format



Project Home

[Downloads](#)

[Wiki](#)

[Issues](#)

[Source](#)

[Export to GitHub](#)

Summary [People](#)

Project Information

★ Starred by 1126 users

[Project feeds](#)

Code license

[New BSD License](#)

Labels

[smali](#), [baksmali](#), [Android](#),
[dalvik](#), [dexformat](#),
[assembler](#), [disassembler](#)



Members

jesusfreke@jesusfreke.com,

bgruv@google.com

[1 contributor](#)

Featured



Downloads

[baksmali](#)

[baksmali-2.0.3.jar](#)

[smali-2.0.3.jar](#)

[Show all »](#)

About

smali/baksmali is an assembler/disassembler for the dex format used by dalvik, Android's Java VM implementation. The syntax is loosely based on Jasmin's/dedexer's syntax, and supports the full functionality of the dex format (annotations, debug info, line info, etc.)

The names "smali" and "baksmali" are the Icelandic equivalents of "assembler" and "disassembler" respectively. Why Icelandic you ask? Because dalvik was named for an Icelandic fishing village.

Curious what the smali format looks like? Here's a quick [HelloWorld example](#) to whet your appetite.

Got questions/comments? Need help? Come hang out in [#smali](#) on freenode.

News

2015-04-30 v2.0.6 is out! Bugfixes, etc.

- Fixes a bug with parameter annotations (credit: Jiri Hrushka)
- Improves the build experience when dx is not on path
- baksmali should be working correctly on windows 8.1 now
- Fixes for the deodexerant makefile (credit: Victor Kaiser-Pendergrast)
- Various other bugfixes, etc. (thanks to Rover12421 for a handful of small fixes)

2015-01-20 v2.0.5 is out! It fixes a multi-threading issue in baksmali in 2.0.4, and it switches the default for implicit references to no-implicit-references, for better backwards compatibility.

Smali Assembly Byte Code

Classes.dex

smali.jar

```
.method protected onCreate(Landroid/content/Context;Landroid/os/Bundle;)V
    .registers 8

    const/4 v3, 0x0

    const/4 v2, 0x1

    invoke-super {p0, p1}, Landroid/app/Activity;.<init>()V

    const v0, 0x7f04001b

    invoke-virtual {p0, v0}, Lcom/shen/app/MainActivity;.<init>()V

    invoke-direct {p0}, Lcom/shen/app/MainActivity;.<init>()V

    move-result v0

    if-nez v0, :cond_12

    :goto_11
    return-void

    :cond_12
    invoke-virtual {p0}, Lcom/shen/app/MainActivity;.<init>()V

    move-result-object v0

    invoke-virtual {v0}, Landroid/content/Context;.<init>()V
```

Smali Assembly Byte Code

```
.method protected onCreate(Landroid/oc
    .registers 8

    const/4 v3, 0x0

    const/4 v2, 0x1

    invoke-super {p0, p1}, Landroid/s

    const v0, 0x7f04001b

    invoke-virtual {p0, v0}, Lcom/shen/a

    invoke-direct {p0}, Lcom/shen/a

    move-result v0

    if-nez v0, :cond_12

    :goto_11
    return-void

    :cond_12
    invoke-virtual {p0}, Lcom/shen/a

    move-result-object v0

    invoke-virtual {v0}, Landroid/cor
```

baksmali.jar

Classes.dex



*But...Smali Bytecode Is Too much,
Could We Find Important Info In Short Time?*



唐鳳

@audreyt



Following

@clkao @ETBlue @evenwu 講個秘訣：講
「講個秘訣前，先講講個秘訣，再講秘訣」
前，先講「講個秘訣：講『講個秘訣前，先
講講個秘訣，再講秘訣』前，先講『講個秘
訣』，再講『講個秘訣前，先講講個秘訣，
再講秘訣』」，再講「講個秘訣前，先講講
個秘訣，再講秘訣」。



pxb1988 / dex2jar

Watch

44

★ Star

357

Fork

98

Tools to work with android .dex and java .class files

<> Code

Issues

15

Pull requests

1

Wiki

Pulse

Graphs

HTTPS clone URL

https://github.com



You can clone with [HTTPS](#) or [Subversion](#).

Clone in Desktop

Download ZIP

489 commits

2 branches

30 releases

2 contributors



branch: 2.x

dex2jar / +

remove println



pxb1988 authored 15 days ago

latest commit 1020541e3c



d2j-base-cmd	shutup compiler	a month ago
d2j-j6	support git/hg revision in meta-info	2 months ago
d2j-jasmin	shutup compiler	a month ago
d2j-smali	fix compiler error by perv commit	15 days ago
dex-ir	fix	a month ago
dex-reader-api	Goodbye googlecode, thanks for the hosting	3 months ago
dex-reader	fix compiler error in generating asmifier of dex file	a month ago
dex-tools	fix compiler error by perv commit	15 days ago
dex-translator	remove println	15 days ago
	use antlr4 to parse smali files	15 days ago

Dex2Jar



Dex2Jar

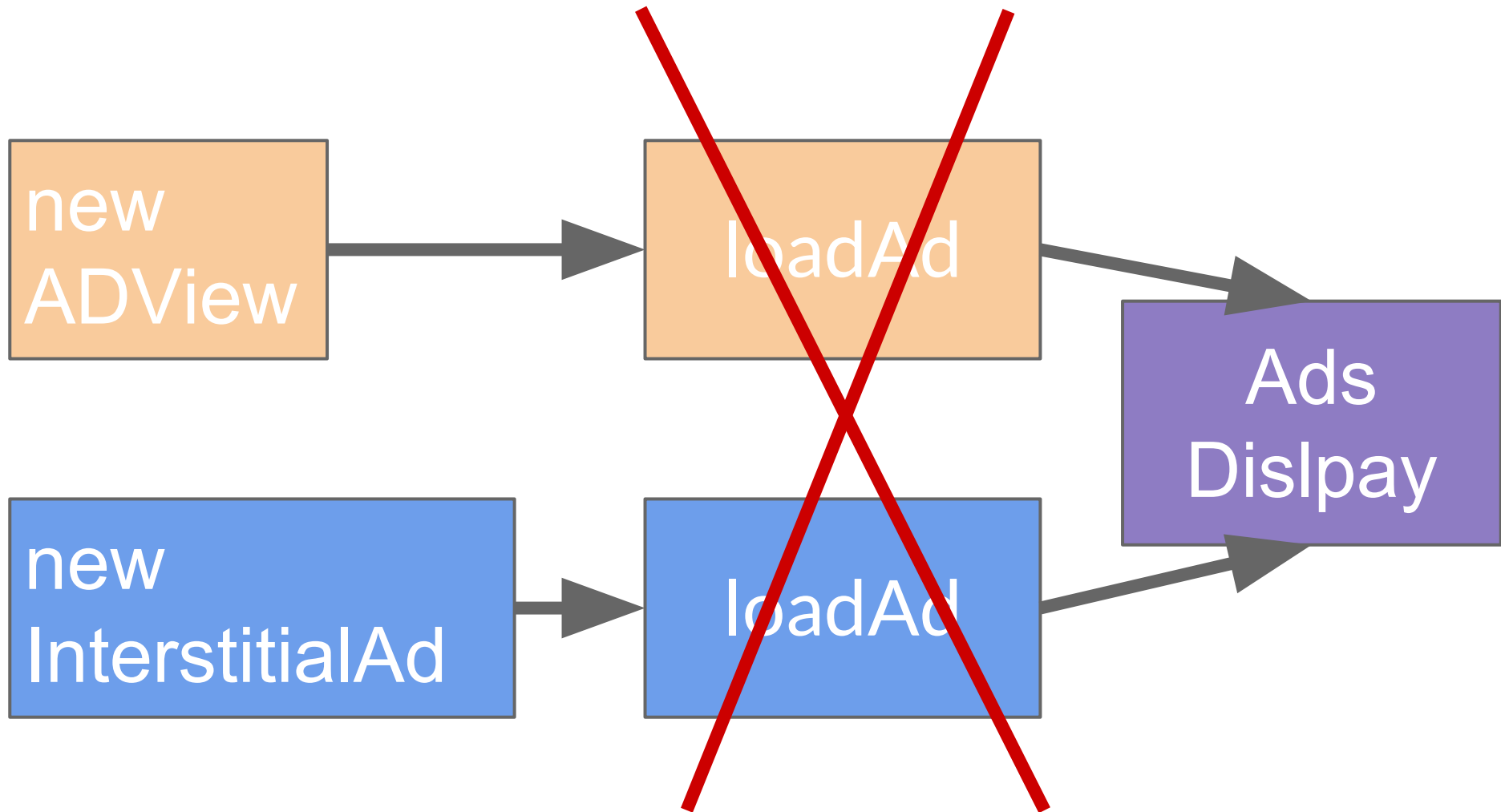
Jar

Jd-Gui.exe

```
    {
        str1 = localTypedValue.string.toString();
        if ((!paramBoolean) || (str1 != null))
            break label275;
        throw new com.google.ads.internal.b("Required XML attribute \""
    }
}
catch (Resources.NotFoundException localNotFoundException)
{
    throw new com.google.ads.internal.b("Could not find resource for
}
throw new com.google.ads.internal.b("Resource " + paramString + " w
label275: return str1;
}

private boolean b(Context paramContext, AdSize paramAdSize, Attribute
{
    ...il.b(paramContext))
    ...context, "You must have INTERNET and ACCESS_NETWORK_STATE
    ...false;
}
return true;
}

private Set<String> c(String paramString, Context paramContext, Attri
throws com.google.ads.internal.b
{
    String str1 = b(paramString, paramContext, paramAttributeSet, param
    HashSet localHashSet = new HashSet();
    if (str1 != null)
    {
        String[] arrayOfString = str1.split(",");
        int i = arrayOfString.length;
        ...
    }
}
```

```

.method public loadAd(Lcom/google/ads/AdRequest;)V
    .registers 3
    .param p1, "adRequest"    # Lcom/google/ads/AdRequest;

    .prologue
    .line 605
    inst-object v0, v0, Lcom/google/ads/AdView; .s Lcom/google/ads/internal/d

public void loadAd(AdRequest paramAdRequest)
{
    if (this.a == null)
        return;
    if (isRefreshing())
        this.a.e();
    this.a.a(paramAdRequest);
}

    .line 613
    :cond_14
    return-void
.end method

```

Prevent loadAd()

1. Find Out All Codes Calling loadAd() ,And Patching Those.
2. Clear All Code Of loadAd() , Let It Be An Empty Function.

So..We Can... do it this way

```
public void loadAd(AdRequest paramAdRequest)
{

}

}
```

Smali Function

Basic Architecture

```
.method public FuncName( ... path... )V/Z/B/S/I/C/J/F/D
    .registers VariableCount
    .param p1, "adRequest"    #Lcom/google/ads/AdRequest;
    .prologue

    return-void
.end method
```

```
.method public loadAd(Lcom/google/ads/AdRequest;)V
  .registers 3
  .param p1, "adRequest"    # Lcom/google/ads/AdRequest;
```

```
    return-void
.end method
```

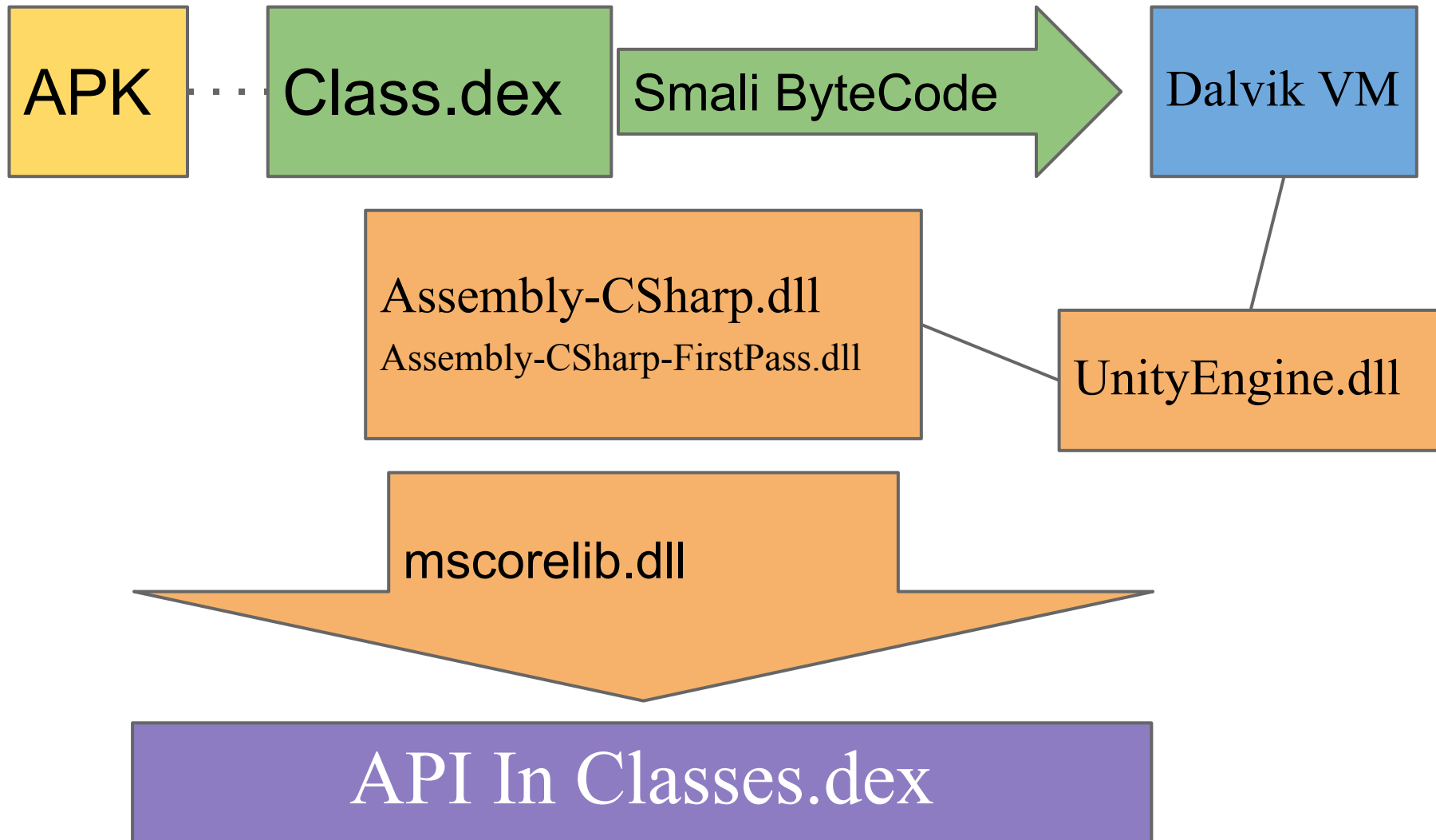


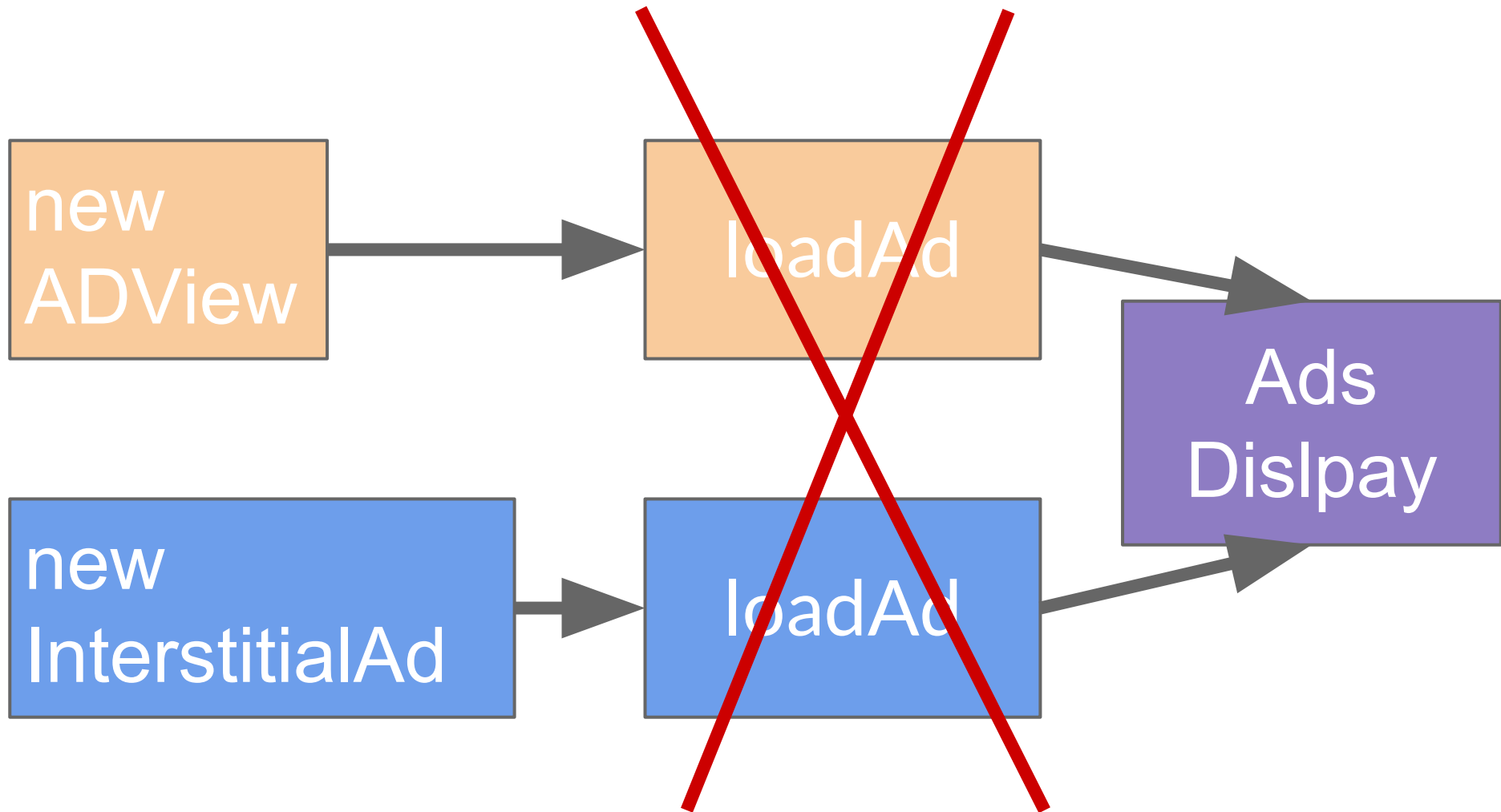
Demo : Patch Ads



Ads In Unity

Unity Works On Android









ProGuard Obfuscation



*Android Basic Cracking Is Easy And Fun,
Until...*

ProGuard



“

$$1+1 = 2$$

Source Code Do = What Will Happen



“



$$1+1+\textcolor{red}{1}-\textcolor{red}{1} = 2$$



$[2 * (1+1-7) * (-1) / 10] * (4 > 1) = 2$

*Source Code Do = What Will Happen
(ProGuard Do Obfuscation)*

- AdView
 - AdView
 - a : d
 - AdView(Activity, AdSize, String)
 - AdView(Activity, AdSize[], String)
 - AdView(Context, AttributeSet)
 - AdView(Context, AttributeSet, int)
 - a(Activity, AdSize, String) : void
 - a(AdSize[]) : void
 - a(Context, AdSize, AttributeSet) : boo
 - a(Context, AttributeSet) : void
 - a(Context, String, AdSize, AttributeSet
 - a(Context, String, int, AdSize, Attribute
 - a(Context, int) : int
 - a(String) : AdSize[]
 - a(String, AttributeSet) : boolean
 - a(String, Context, AttributeSet, boolex
 - b(Context, AdSize, AttributeSet) : boo
 - b(String, Context, AttributeSet, boolex
 - c(String, Context, AttributeSet, boolex
 - destroy() : void
 - isReady() : boolean
 - isRefreshing() : boolean
 - loadAd(AdRequest) : void
 - onMeasure(int, int) : void
 - setAdListener(AdListener) : void
 - setAppEventListener(AppEventListene
 - setSupportedAdSizes(AdSize[]) : void
 - stopLoading() : void

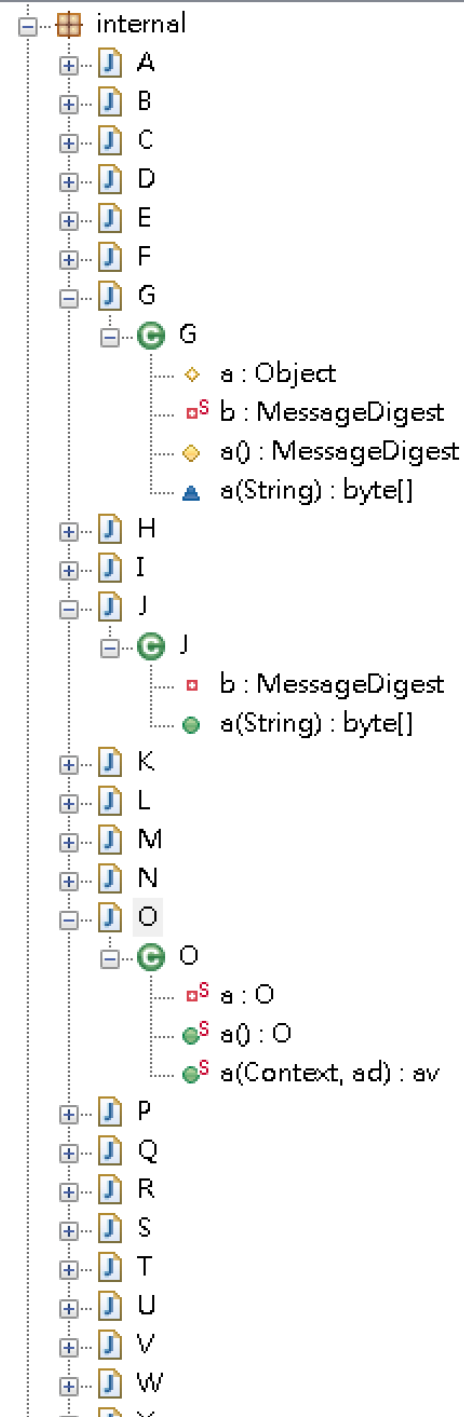
- android.gms
 - a
 - ads
 - a
 - b
 - c
 - AdActivity
 - AdView
 - AdView
 - a : af
 - AdView(Context)
 - AdView(Context, AttributeSet)
 - AdView(Context, AttributeSet, int)
 - a() : void
 - a(String) : void
 - a(a) : void
 - a(b) : void
 - a(d) : void
 - b() : void
 - c() : void
 - onLayout(boolean, int, int, int, int) : void
 - onMeasure(int, int) : void
 - a
 - b
 - c
 - d
 - e
 - common
 - internal
 - a

```
public void loadAd(AdRequest paramAdRequest)
```

```
{  
    if (this.a == null)  
        return;  
    if (isRefreshing())  
        this.a.e();  
    this.a.a(paramAdRequest);  
}
```



Fucking Code Review



```

public final void a(ad paramad)
{
    try
    {
        if (this.d == null)
        {
            if (((this.e == null) || (this.f == null))) && (this.d == null))
                throw new IllegalStateException("The ad size and ad unit ID must be set before loadAd is called.");
            Context localContext = this.g.getContext();
            this.d = M.a(localContext, new ay(localContext, this.e), this.f, this.a);
            if (this.c != null)
                this.d.a(new L(this.c));
            e();
        }
        if (!this.d.a(Q.a(this.g.getContext(), paramad)))
            return;
        this.a.a(paramad.i());
        return;
    }
    catch (RemoteException localRemoteException)
    {
    }
}

```

```
public final void a(ad paramad)
{
    try
    {
        if (this.e == null)
        {
            if (this.f == null)
                b("loadAd");
            this.e = M.a(this.b, new ay(), this.f, this.a);
            if (this.d != null)
                this.e.a(new L(this.d));
        }
        if (this.e.a(Q.a(this.b, paramad)))
            this.a.a(paramad.i());
        return;
    }
    catch (RemoteException localRemoteException)
    {
    }
}
```

ProGuard Obfuscation Property

1. Type Name Will Keep Intact.
2. Only Confuse The Functions Used In App.
3. Add A New Type Named “Internal”.
4. Functions Will Be Translated Into Lots Of Pieces Put In Internal Type.
5. Would Not Confuse String In Function.

How To Analytics Code In ProGuard

1. Dynamic Debug And Trace Code In App.



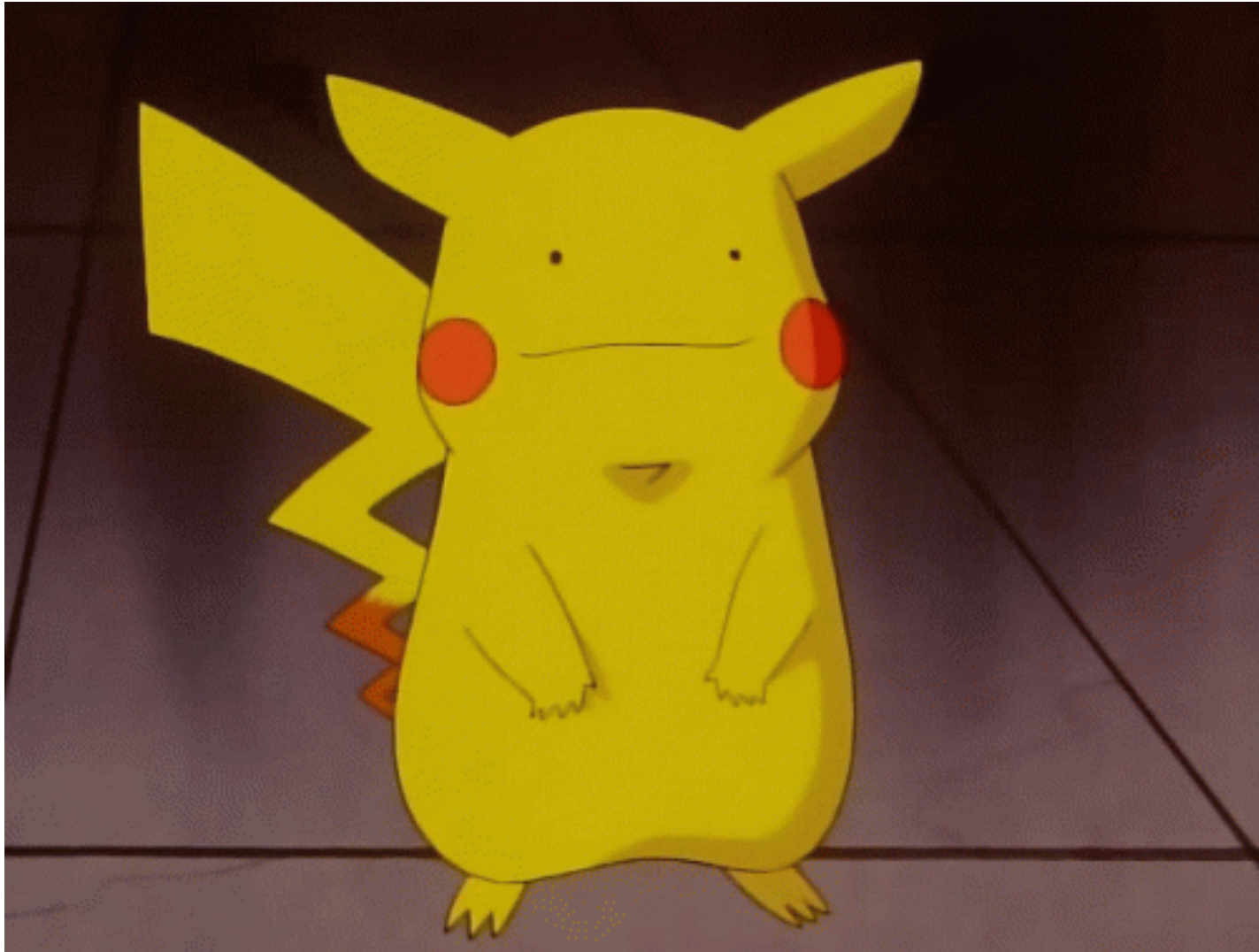
How To Analytics Code In ProGuard

2. Review Obfuscation Codes.



How To Analytics Code In ProGuard

3. De-Obfuscation (If Possible?)





How To Build AIDS Tool In C#

How To Clear Ads In APK.

Protected By ProGuard Obfuscation Or Not

1. Extract Classes.dex From Ads
2. Translate Classes.dex To Smali Asm Code
3. Find The loadAd() And Empty It (If Protected By ProGuard,Need To Check All Functions In Intent Type)
4. Translate Smali Asm Code Back To .Dex
5. Package All Data To ZIP Package
6. Sign The ZIP And Name It As .APK



[adamhathcock](#) / **sharpcompress**

Watch

33

Star

133

Fork

58

SharpCompress is a fully managed C# library to deal with many compression types and formats.

<http://sharpcompress.codeplex.com>

170 commits

6 branches

9 releases

15 contributors



branch: master ▾

sharpcompress / +



Update license URL



Adam Hathcock authored 16 days ago

latest commit [9eb43156e8](#)

NuGet	Update license URL	16 days ago
SharpCompress.Test	Made unsigned csproj for testing. Sign the main DLL again.	16 days ago
SharpCompress	Update for 0.11	16 days ago
TestArchives	Fixed bug causing entries of non-ustar archive being after one with v...	6 months ago
packages	Added .NET 2.0 version (with LinqBridge)	a year ago
.gitignore	Added .NET 2.0 version (with LinqBridge)	a year ago
LICENSE.txt	Adds MIT license.	8 months ago
README.md	Update for 0.11	16 days ago

<> Code

Issues

23

Pull requests

0

Wiki

Pulse

Graphs

HTTPS clone URL

<https://github.com>

You can clone with [HTTPS](#) or [Subversion](#). ⓘ

Clone in Desktop

Download ZIP



smali

An assembler/disassembler for Android's dex format



Project Home

[Downloads](#)

[Wiki](#)

[Issues](#)

[Source](#)

[Export to GitHub](#)

Summary [People](#)

Project Information

★ Starred by 1126 users

[Project feeds](#)

Code license

[New BSD License](#)

Labels

smali, baksmali, Android,
dalvik, dexformat,
assembler, disassembler



Members

jesusfreke@jesusfreke.com,

bgruv@google.com

[1 contributor](#)

Featured



Downloads

[baksmali](#)

[baksmali-2.0.3.jar](#)

[smali-2.0.3.jar](#)

[Show all »](#)

About

smali/baksmali is an assembler/disassembler for the dex format used by dalvik, Android's Java VM implementation. The syntax is loosely based on Jasmin's/dedexer's syntax, and supports the full functionality of the dex format (annotations, debug info, line info, etc.)

The names "smali" and "baksmali" are the Icelandic equivalents of "assembler" and "disassembler" respectively. Why Icelandic you ask? Because dalvik was named for an Icelandic fishing village.

Curious what the smali format looks like? Here's a quick [HelloWorld example](#) to whet your appetite.

Got questions/comments? Need help? Come hang out in [#smali](#) on freenode.

News

2015-04-30 v2.0.6 is out! Bugfixes, etc.

- Fixes a bug with parameter annotations (credit: Jiri Hrushka)
- Improves the build experience when dx is not on path
- baksmali should be working correctly on windows 8.1 now
- Fixes for the deodexerant makefile (credit: Victor Kaiser-Pendergrast)
- Various other bugfixes, etc. (thanks to Rover12421 for a handful of small fixes)

2015-01-20 v2.0.5 is out! It fixes a multi-threading issue in baksmali in 2.0.4, and it switches the default for implicit references to no-implicit-references, for better backwards compatibility.



signapk

onboard apk signing script for android devices

[Project Home](#)[Downloads](#)[Wiki](#)[Issues](#)[Source](#)[Export to GitHub](#)[Summary](#) [People](#)

Project Information



Starred by 37 users

[Project feeds](#)

Code license

[GNU GPL v2](#)

Labels

Android, signapk,
Embedded



Members

[atomicdryad](#)

Usage: signapk (options) [command] (files)

commands:

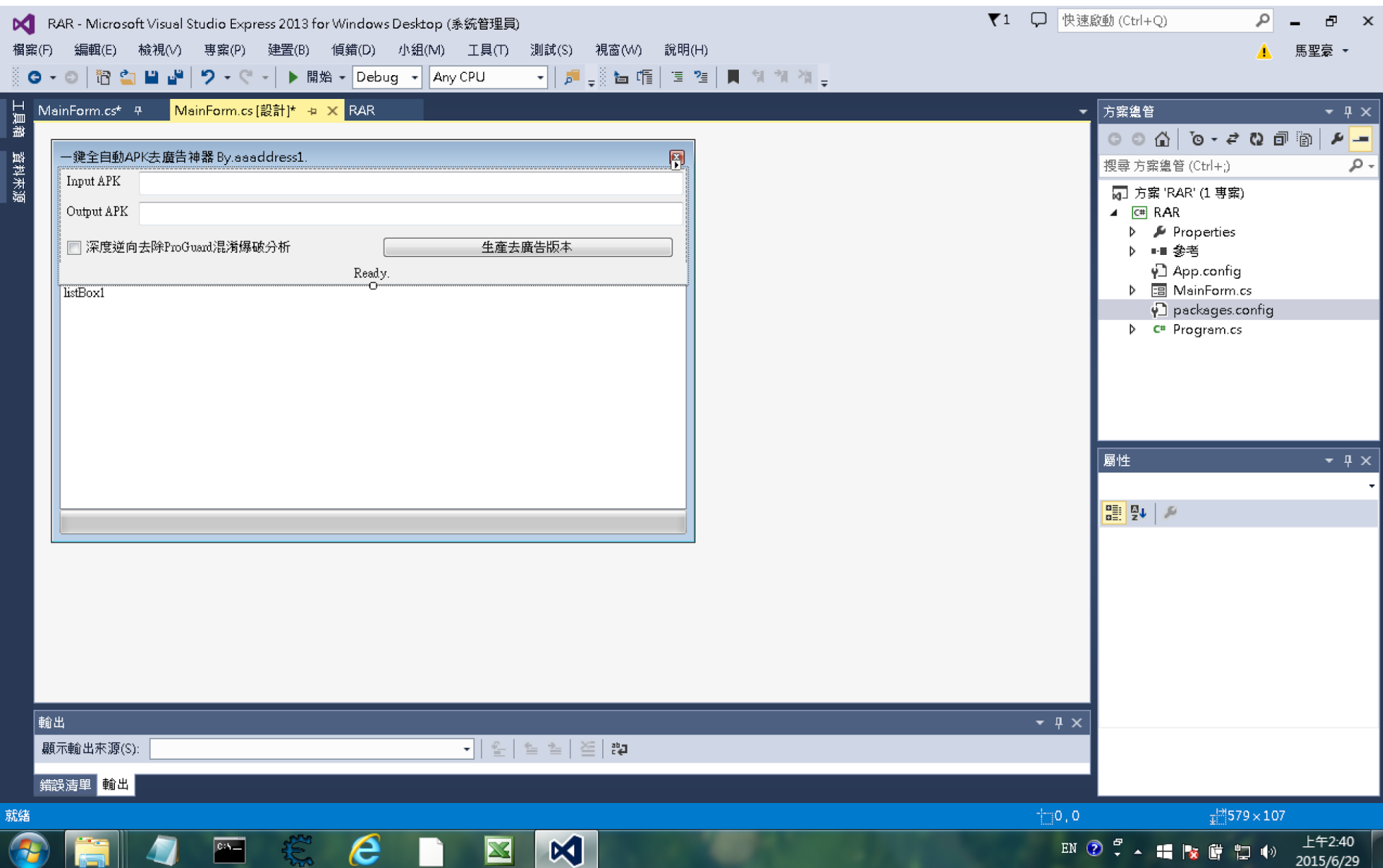
sign FILE	sign a .zip or .apk
sign FILE1 FILE2	create a signed copy of FILE1 as FILE2
cert FILE(s)	print cert info on FILE's signer
certinfo FILE	print detailed cert info on FILE's signer
cmp FILE	compare signer of FILE with default/selected cert
cmp FILE1 FILE2	compare signer of FILE1 to signer of FILE2

options:

-k, --key FILE	key to sign with
-c, --cert FILE	cert to sign with
	if -c or -k are not files then they are considered aliases to builtins (ie -k testkey or -c platform)
-f, --force	sign even if cert differs from original
-t, --tmp DIR	use DIR for tempdir instead of '/cache'
-d, --debug	output debugging
-V, --version	print 'signapk v0.3.1'

exit codes:

1: read error (file 1)	2: read error (file 2)
3: write error	4: ssl error
5: zip write error	9: key error
8: sign: cert mismatch	10: cmp: cert mismatch
128: script error	255: user error



```
private void GetFiles(DirectoryInfo di, string searchPattern, ref ArrayList MyFiles)
{
    try
    {
        foreach (FileInfo fi in di.GetFiles(searchPattern))
        {
            MyFiles.Add(fi.FullName);
        }
        foreach (DirectoryInfo d in di.GetDirectories())
        {
            GetFiles(d, searchPattern, ref MyFiles);
        }
    }
    catch (Exception)
    {
    }
}
```

```

int DeepFuckFuncContentText(string SmaliPath, string ContentText)
{
    string Source = (File.ReadAllText(SmaliPath));
    int FuckStrPos = Source.IndexOf(ContentText);
    if (FuckStrPos < 0) return (-1);

    int AdsFuncStartPos = Source.LastIndexOf(".method", FuckStrPos);
    int AdsFuncEndPos = Source.IndexOf(".end method", FuckStrPos);
    string AdsSource = (Source.Substring(AdsFuncStartPos, AdsFuncEndPos - AdsFuncStartPos));

    string PatchedBannerSource = "";
    foreach (var item in AdsSource.Split('\n'))
    {
        if (item.Length < 1) continue;
        if (new Regex(@".*?\s.method\s.*?").IsMatch(item)) PatchedBannerSource += item + "\r\n";
        if (new Regex(@".*?\s.registers.*?").IsMatch(item)) PatchedBannerSource += item + "\r\n";
        if (new Regex(@".*?\s.prologue.*?").IsMatch(item)) PatchedBannerSource += item + "\r\n";
        if (new Regex(@".*?\s.const\:\/\/.*?").IsMatch(item)) PatchedBannerSource += item + "\r\n";
        if (new Regex(@".*?\sreturn\s(-void|\s\w).*?").IsMatch(item)) PatchedBannerSource += item + "\r\n";
    }
    Source = Source.Remove(AdsFuncStartPos, AdsFuncEndPos - AdsFuncStartPos);
    Source = Source.Insert(AdsFuncStartPos, PatchedBannerSource);
    File.WriteAllText(SmaliPath, Source);
    return AdsFuncStartPos;
}

```

一鍵全自動APK去廣告神器 By.aaaddress1.

Input APK C:\Users\aaaddress1\Desktop\AutoPatchAds\RAR\RAR\bin\Debug\南臺學生助理.1.0.apk

Output APK C:\Users\aaaddress1\Desktop\AutoPatchAds\RAR\RAR\bin\Debug\南臺學生助理.1.0_ADS_Fuck.apk

☒ 深度逆向去除ProGuard混淆爆破分析

生產去廣告版本

完成!

開始初始化工作.

開始解析APK.

開始逆向APK回Smali.

開始找尋所有可逆向分析之結構.

開始逆向分析..

- [受混淆保護廣告]	out\com\google\android\gms\internal\af.2.smali	patched at 7733
- [受混淆保護廣告]	out\com\google\android\gms\internal\ag.2.smali	patched at 4216
- [受混淆保護廣告]	out\com\google\android\gms\internal\dE.smali	patched at 1280
- [受混淆保護廣告]	out\com\google\android\gms\internal\fl.smali	patched at 82585

一共發現了 4 處程式碼含有廣告(程式已修補完成).

正在將修改點包回程式核心.

正在將APK包回原始軟體壓縮包.

正在替APK重新簽章.

完成!



Demo AIDS

Hello!

aaaddress1(ADR)

Q&A

aaaddress1@gmail.com

