
一步登天
零基礎無痛入門APK逆向
Hack Stuff Technology聚會
By ADR

0x00_自我介紹;

馬聖豪(ADR)
義守大學

資工大一新生 ψ(`▽´)ψ
aaaddress1@gmail.com

aaad

aaaddress1
aaad
aaad prague
aaaddress1神魔
aaadvantage
aaa digital
aaadvantage dining
aadvantage mall
cadd9
admin

Google 搜尋　好手氣

訂閱人數：107　觀看次數：324,755　影片管理員　觀眾看到的畫面

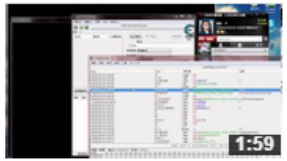
聖豪馬

首頁　影片　播放清單　頻道　討論　簡介

上傳　新增日期 (最新 - 最舊)

第一次手拆非常好厂幺°色6就上手

觀看次數：7 • 3 個月前



POE_multi-CreateGame

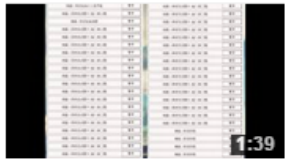
• 觀看次數：18 • 3 個月前

自幹FaceBook Messenager For Windows

觀看次數：394 • 5 個月前

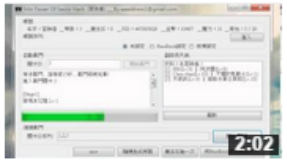
無限HP

觀看次數：597 • 1 年前



神魔之塔無限首抽

觀看次數：6,903 • 1 年前

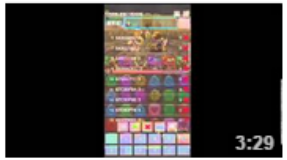


無限首抽

觀看次數：5,458 • 1 年前

神魔之塔靚機自動戰鬥

• 觀看次數：102 • 1 年前



神魔之塔 改Combo傷害

• 觀看次數：531 • 1 年前

MyCandy! CandyCrush Cheat

觀看次數：330 • 1 年前

FaceBook Token Inject To Login Bypass Password.

觀看次數：1,251 • 1 年前

Vb.net 程式自動復活

觀看次數：647 • 1 年前

前鎮高中205-第四組-生活科技影片(小高雄大故事)

觀看次數：280 • 2 年前

Search GitHub

Explore Gist Blog Help

aaaddress1

馬聖豪
aaaddress1

Taiwan
aaaddress1@gmail.com
http://helloadr.blogspot.tw/
Joined on 27 Aug 2014

11	0	7
Followers	Starred	Following

Contributions | Repositories | Public activity

Edit profile

Popular repositories

FkBBTalk 3
剃除該死的聊聊

CSharp-Hosts-HTTP-Hook 1
酷狗音樂破解

AdrEngine-MapleStory-In-VB.... 0
以VB.NET開發的一套全智能搜索楓之谷線上遊戲記憶體的分析引擎.

DLL-Injector-In-VB.NET 0
以VB.NET實作CreateThread做LoadLibraryA遠程注入DLL.

Replace-ModuleInfo-From-PE... 0
將指定模組的記憶體名字從PE Header上抹除/替換,但保留模組可存在於進程內存活.

Contributions

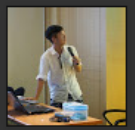
Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec Jan

M
W
F

ADR's拆拆手札

狂人手札，記錄生活中的麻煩事

關於我自己



聖豪馬

追蹤

Hi,我是ADR(aaaddress1)
專長在Windows上分析逆向各種商業軟體.
擅長語言C++、Visual Basic、C#、MASM8086、QT、Python

檢視我的完整簡介

總瀏覽量

3,811

+1 0

標籤

- .NET (2)
- APK (1)
- ASM (1)
- C++ (2)
- CBuilder (2)
- CheatEngine (2)
- Chrome (2)
- Crack (5)
- Debugger (1)

Google+ Followers

聖豪馬

加到社交圈

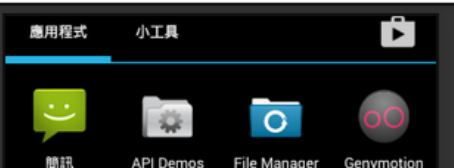
2015年2月4日 星期三

初探手工爆破逆向Apk（反編＋打補釘＋回簽）

為什麼會有這一篇呢？...因為某逼巴ADR想學學Apk怎麼逆向XD
好歹逆向在Windows上也不算太嫩但感覺技能遲遲無法拿上手機Apk逆向有點雷啊XD

參考文獻：
http://blog.sina.com.cn/s/blog_70677d110100xzht.html
http://blog.csdn.net/lucherr/article/details/39896549

首先
本文主角是這個XD
網路上找來練習逆向的小入門Apk
下載點我點我點我



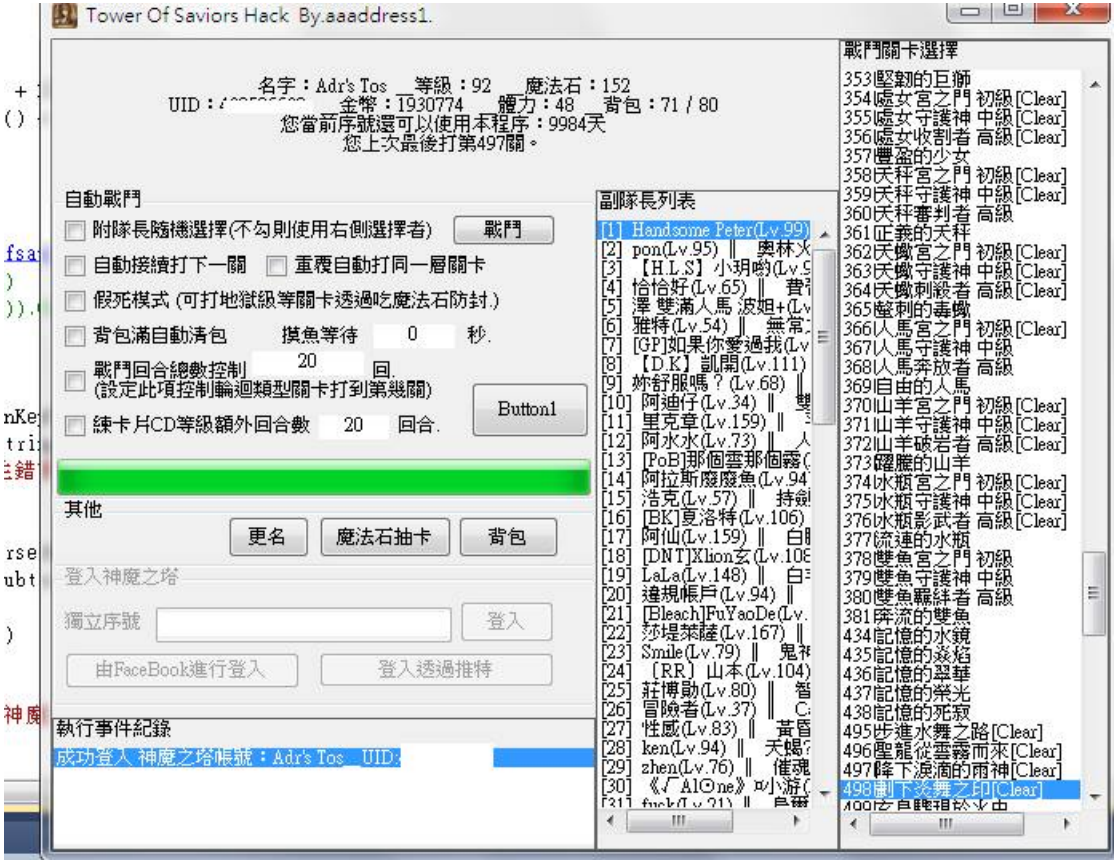
MapleHack


楓之谷駭客功能表單 For Twms.v.1.7
楓之谷 駭客。
MAPLE HACK!
遊戲功能表單
駭客註解說明欄(有特別解說將會顯示於此)
一般功能
實用功能
強化功能
隱藏界面
全智30%
遠攻不揮弓
僵屍怪物
無敵八秒
怪物不反擊
人物不被擊退
物理無敵
強化五次MISS
無限日標
超級撿物
怪物完全KB
怪物不被擊退
完成驗證
駭客介紹員
Ver. 1.7
MapleStory
帳號
密碼
登入
記憶帳號
查詢帳號
查詢密碼
小鍵盤
楓之谷駭客-MapleHack-(完成登入)
楓之谷駭客
隱藏駭客
自動按鍵
登入駭客
關閉駭客
maplehackvip.blogspot.com/
如何開通?
程式狀態:
完成登入
楓之谷駭客官方網頁

CrackShield

Garena 防爆CPU

小小神魔戰鬥模擬


Tower Of Saviors Hack By.aaaddress1.
名字：Adr's Tos 等級：92 魔法石：152
金幣：1930774 體力：48 背包：71 / 80
您當前序號還可以使用本程序：9984天
您上次最後打第497關。
自動戰鬥
附隊長隨機選擇(不勾則使用右側選擇者)
戰鬥
自動接續打下一關
重覆自動打同一層關卡
假死模式 (可打地獄級等關卡透過吃魔法石防封.)
背包滿自動清包
摸魚等待
0
秒.
戰鬥回合總數控制
20
回.
(設定此項控制輪迴類型關卡打到第幾關)
練卡片CD等級額外回合數
20
回合.
Button1
其他
更名
魔法石抽卡
背包
登入神魔之塔
獨立序號
登入
由FaceBook進行登入
登入透過推特
執行事件紀錄
成功登入 神魔之塔帳號：Adr's Tos UID:
副隊長列表
[1] Handsome Peter(Lv.99)
[2] pon(Lv.95) ‖ 奧林火
[3] 【H.L.S】小玥喲(Lv.9
[4] 恰恰好(Lv.65) ‖ 費
[5] 澤 雙滿人馬 波妲+(Lv
[6] 雅特(Lv.54) ‖ 無常
[7] [GP]如果你愛過我(Lv
[8] 【D.K】凱開(Lv.111)
[9] 妳舒服嗎？(Lv.68) ‖
[10] 阿迪仔(Lv.34) ‖
[11] 里克章(Lv.159) ‖
[12] 阿水水(Lv.73) ‖ 人
[13] [PoB]那個雲那個霧(
[14] 阿拉斯廢廢魚(Lv.94
[15] 浩克(Lv.57) ‖ 持劍
[16] [BK]夏洛特(Lv.106)
[17] 阿仙(Lv.159) ‖ 白
[18] [DNT]Xlion玄(Lv.108
[19] LaLa(Lv.148) ‖ 白
[20] 違規帳戶(Lv.94) ‖
[21] [Bleach]FuYaoDe(Lv.
[22] 莎堤萊薩(Lv.167) ‖
[23] Smile(Lv.79) ‖ 鬼神
[24] 〔RR〕山本(Lv.104)
[25] 莊博勛(Lv.80) ‖ 智
[26] 冒險者(Lv.37) ‖ C
[27] 性感(Lv.83) ‖ 黃昏
[28] ken(Lv.94) ‖ 天蝎
[29] zhen(Lv.76) ‖ 催魂
[30] 《ㄏAlㄛne》ㄖ小游(
[31] fuck(Lv.21) ‖ 皇霸
戰鬥關卡選擇
353堅韌的巨獅
354處女宮之門 初級 [Clear]
355處女守護神 中級 [Clear]
356處女收割者 高級 [Clear]
357豐盛的少女
358天秤宮之門 初級 [Clear]
359天秤守護神 中級 [Clear]
360天秤審判者 高級
361正義的天秤
362天蠍宮之門 初級 [Clear]
363天蠍守護神 中級 [Clear]
364天蠍刺殺者 高級 [Clear]
365蠻刺的毒蠍
366人馬宮之門 初級 [Clear]
367人馬守護神 中級
368人馬奔放者 高級
369自由的人馬
370山羊宮之門 初級 [Clear]
371山羊守護神 中級 [Clear]
372山羊破岩者 高級 [Clear]
373耀麗的山羊
374水瓶宮之門 初級 [Clear]
375水瓶守護神 中級 [Clear]
376水瓶影武者 高級 [Clear]
377流連的水瓶
378雙魚宮之門 初級
379雙魚守護神 中級
380雙魚羈絆者 高級
381奔流的雙魚
434記憶的水鏡
435記憶的炎焰
436記憶的翠華
437記憶的榮光
438記憶的死寂
495步進水舞之路[Clear]
496聖龍從雲霧而來[Clear]
497降下滾滴的雨神[Clear]
498劃下炎舞之印[Clear]

ADR’s FB


粉絲專頁
動態 8
洞察報告
設定
建立粉絲群
使用說明
ADR'S
WWW.FACEBOOK.COM/ADRPLUS
FACEBOOK.
關心、你的朋友們更多一些
Adr's FB 自動按讚、生日快樂、找婊子
應用程式專頁
讚
追蹤中
發訊息
dr's FaceBook
動態時報
關於
說讚的粉絲
相片
更多
本週
244
粉絲專頁的讚
2,707
貼文觸及人數
未讀訊息
3
通知
5
訊息
最新
2014年
2013年
用戶
10,327 個讚
近況
相片/影片
優惠、活動，更多
你都在忙些什麼？
在此查看您的廣告

義守學生管家


Google play
搜尋
+馬
14
應用程式
類別
首頁
熱門排行榜
最新發佈
我的應用程式
購物
遊戲
編輯精選
義守學生管家
馬聖豪 - 2015年3月24日
教育
已安裝
這個應用程式與您的部分裝置相容。
(42)
+1
+2 在 Google 上推薦這個網址
ISU

經歷

- HITCON Junior
- Chroot實習
- TDoH成員

專長&興趣

1) 「玩」遊戲、商業軟體、線上遊戲
2) Windows上的逆向技術
3) 號稱Windows API人肉字典
4) 拼拼裝裝寫出自己的外掛插件
5) VB.NET、C++、MASM、C#
6) 略懂smali、MSIL、Python、JAVA、Ruby、PHP

How to draw A Cat!

1.

2.


哩得工三毀 我攏聽唔

歡迎發問、回答(=ﾟωﾟ)ﾉ

安安,請多給我點互動 ♥

因為這次介紹的是...

新手無痛進入...（？）

新手微痛進入…（O）
APK基礎 → Unity引擎

But講者不是黑客,
也只是略懂略懂<(_ _)>

陳柏宇

別說惹

我是魯蛇黑客

從即時通送出

聽完後你也不一定什麼APK都能拆(尻杯)


LTV
櫻桃小丸子
這個傢伙，一副騙人的嘴臉

因為實作部分很多
Demo
如果NG了，請別笑。要笑請小聲點


很想要吧？

PS：因為本魯學Android App是從破解App開始學der

正所謂學會SQL
就得從SQLi開始學習

如果Slide或者概念上
有任何疑慮都可以說出來

0x01_int main();

逆向APK入門

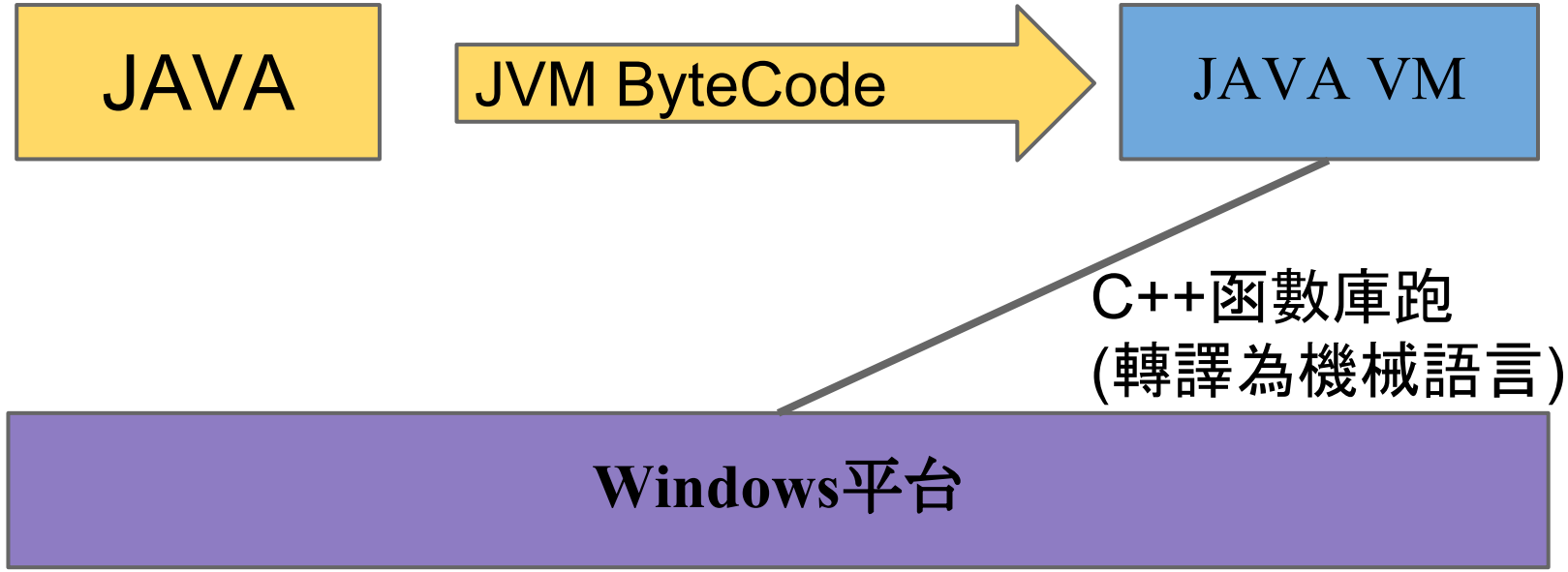
土產工具包

http://goo.gl/OH4vE2

背景知識

標準的Android App是由JAVA語言進行開發的，JAVA在編譯之後會產生中介碼(Bytecode)，執行時由JVM提供的即時編譯(JIT)轉成機械指令，才可以在作業平台上面執行。

Android解析
出Class.dex



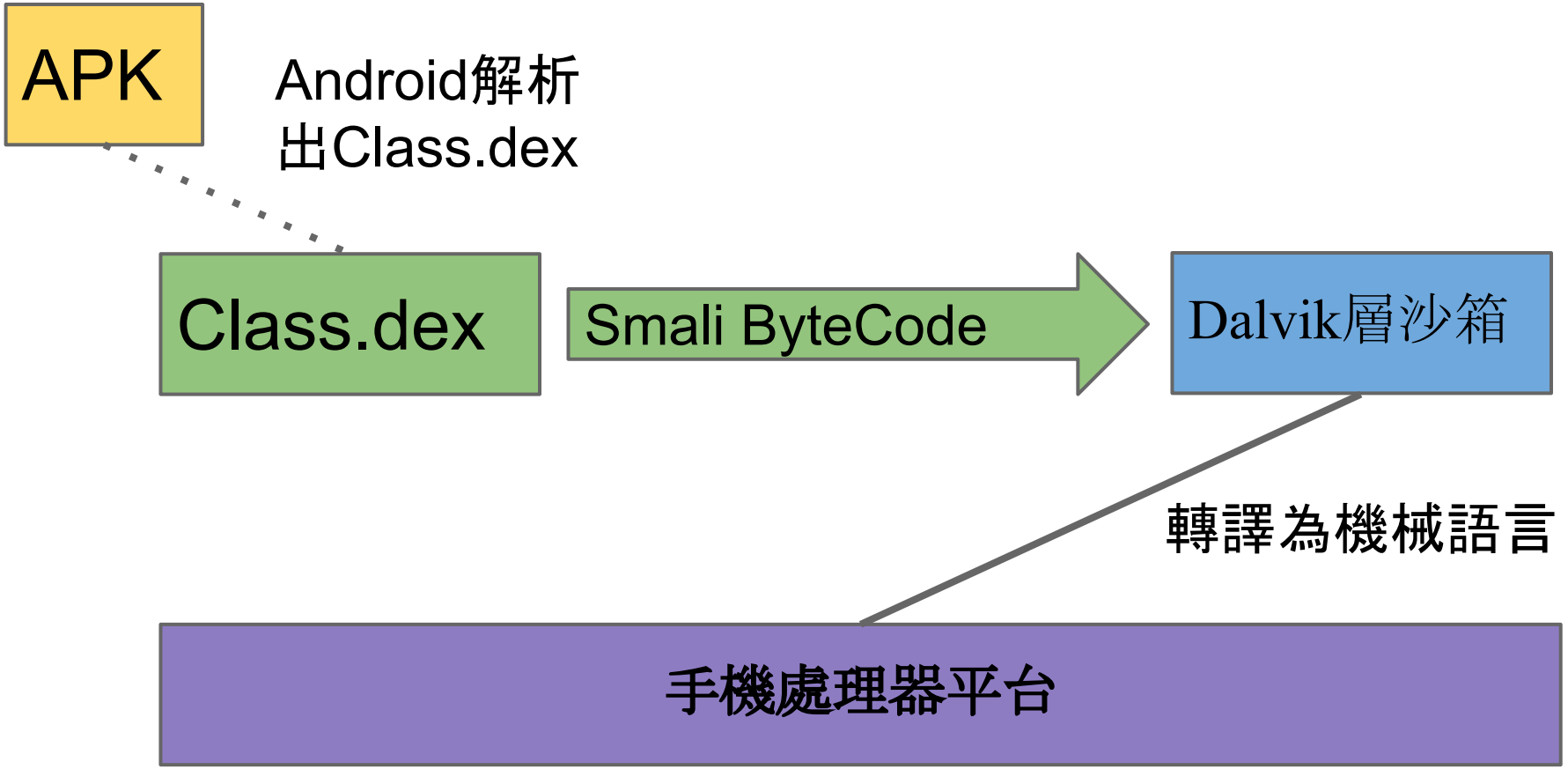
背景知識

也因為這個特性JAVA開發的程式非常容易從中介語言轉回近似甚至完全一樣的原始碼。

那再回來看看Android的App吧！雖然同樣為JAVA寫成,
但是Google在Android平台上所提供的虛擬機器並不是JVM;
而是Dalvik, 透過底層的優化減少虛擬機占用資源以及提高效率等。

背景知識

在Dalvik上通常會以 .apk 的格式提供應用程式的封裝，這些封裝格式主要是用ZIP形式壓縮然後加上相關的參考資訊儲存起來，而我們可以透過反解壓縮.apk檔案你會看到名為classes.dex的檔案，這檔案正是經由編譯器轉換給Dalvik虛擬機看得ByteCode，所以Classes.dex檔就是我們反編譯應用程式的關鍵了!!!


APK
Android解析
出Class.dex
Class.dex
Smali ByteCode
Dalvik層沙箱
轉譯為機械語言
手機處理器平台

那我們該怎麼逆向？

APK那層套子

META-INF

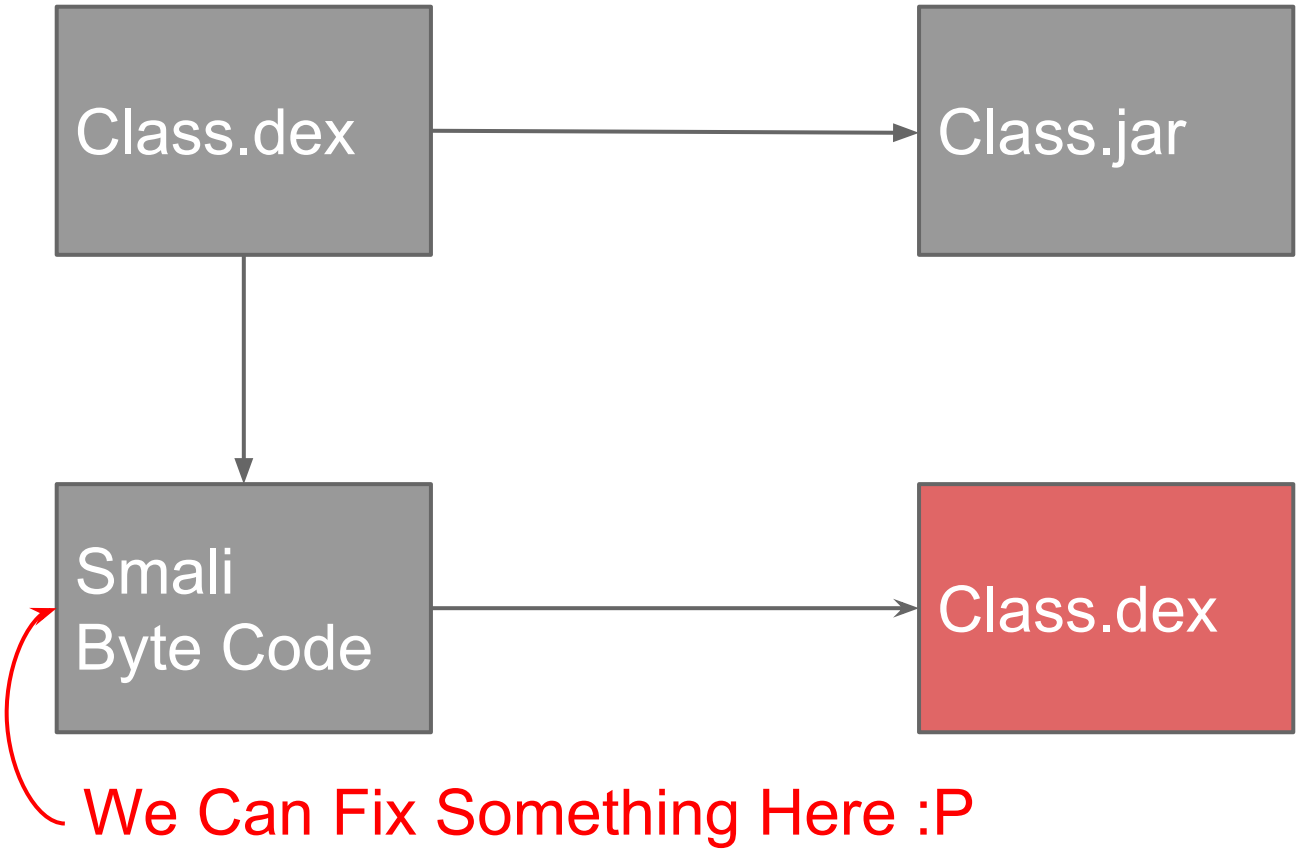
RES

Class.dex

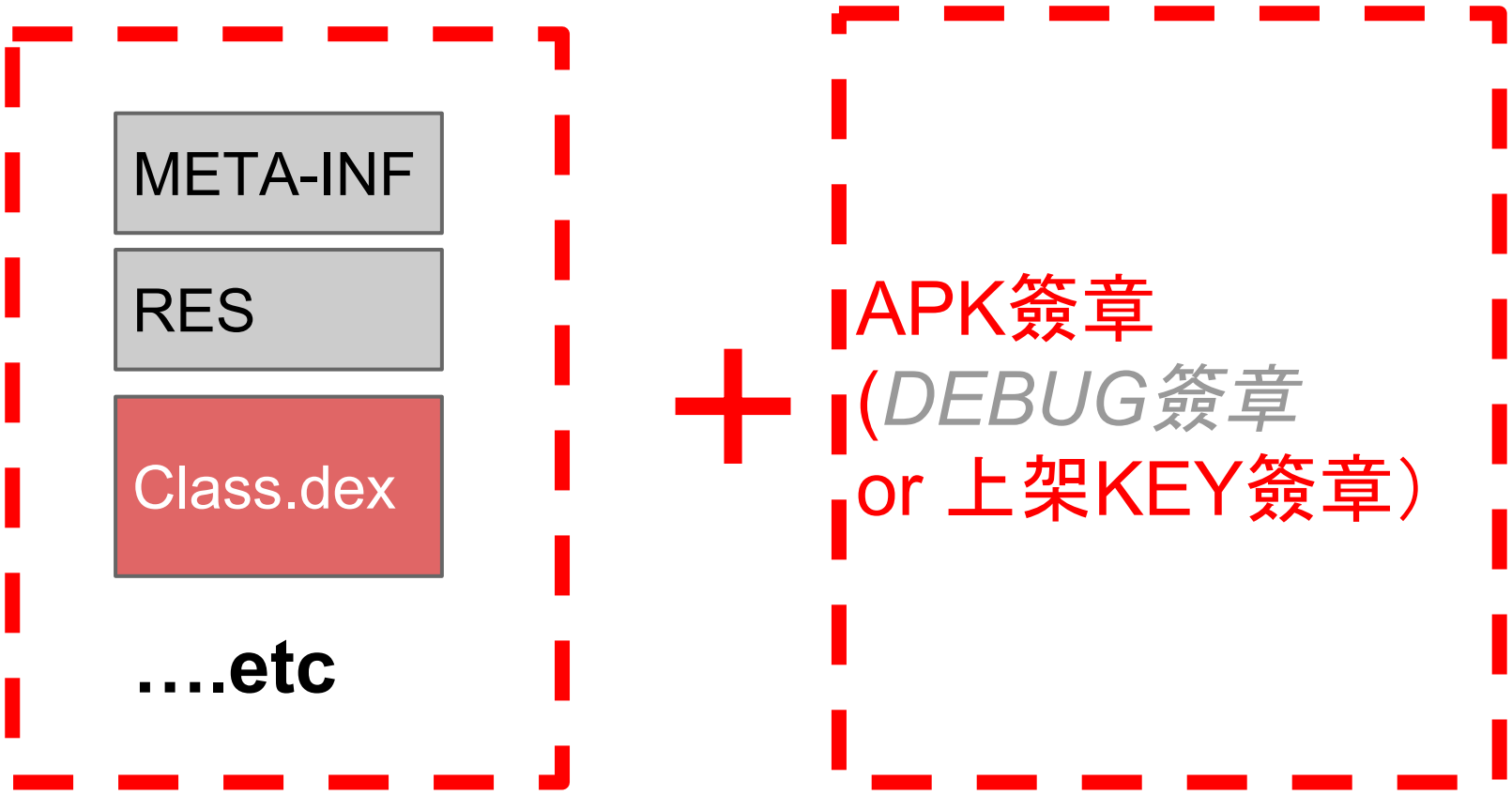
….etc

+

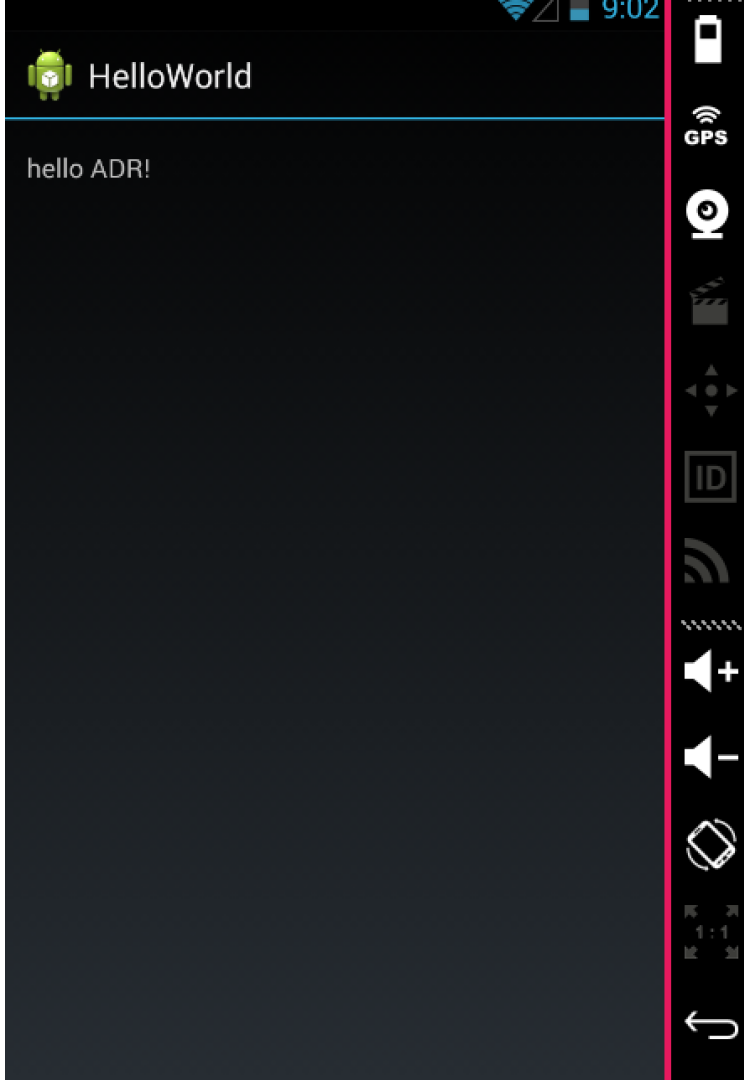
APK簽章
(DEBUG簽章
or 上架KEY簽章)


Class.dex
Class.jar
Smali
Byte Code
Class.dex
We Can Fix Something Here :P

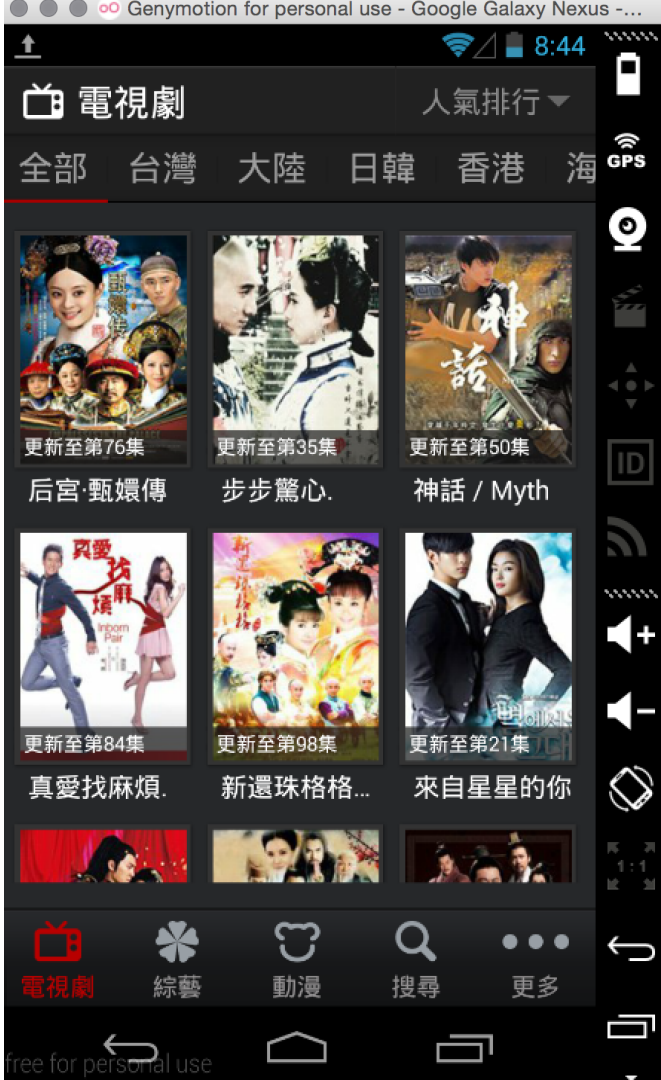
我們得重新替APK套上套子



初探APK逆向！
HelloWorld.apk逆向



網路第四台去啟動廣告

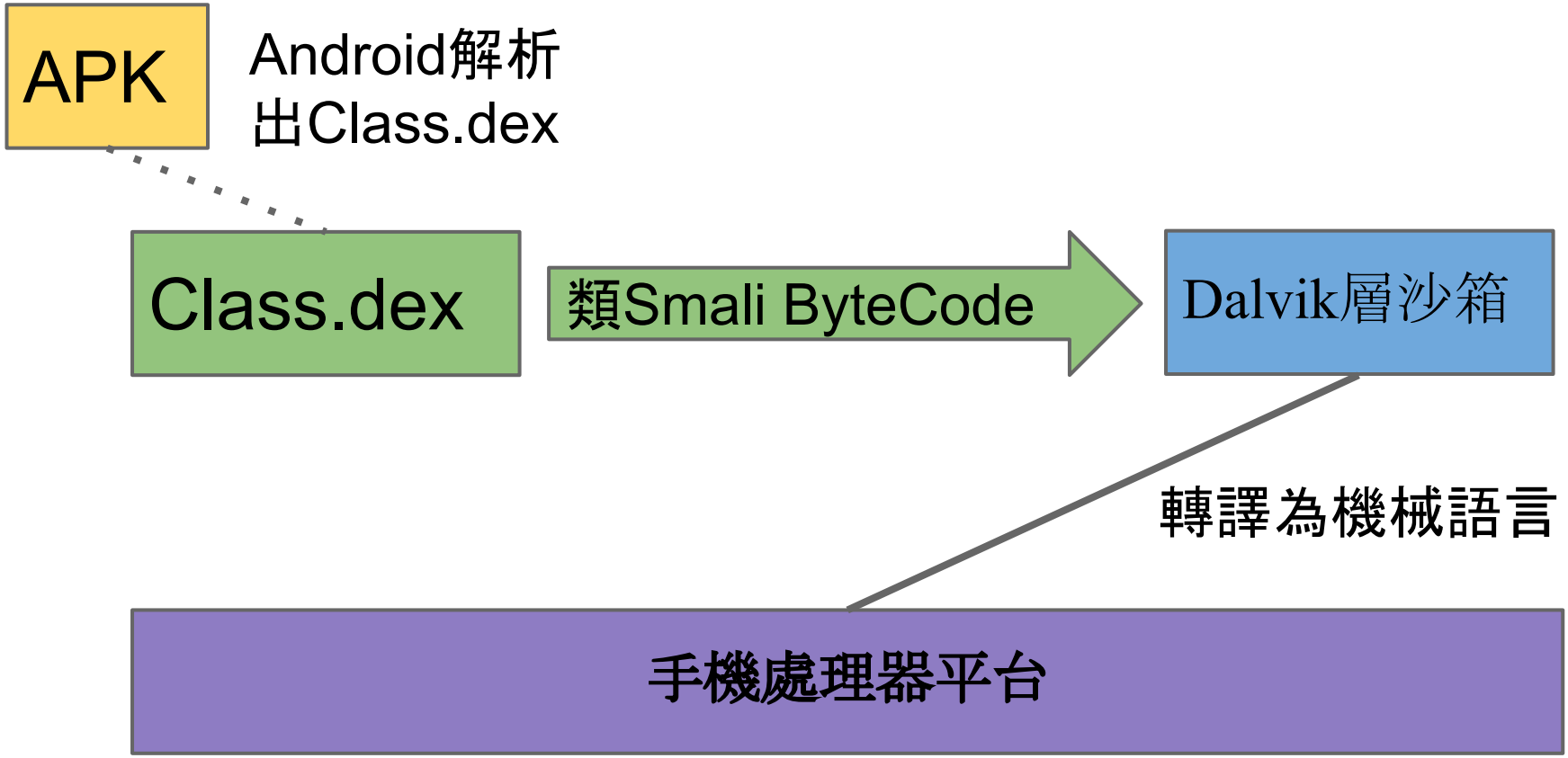

Genymotion for personal use - Google Galaxy Nexus -...
8:44
電視劇
人氣排行
全部
台灣
大陸
日韓
香港
更新至第76集
后宮·甄嬛傳
更新至第35集
步步驚心.
更新至第50集
神話 / Myth
更新至第84集
真愛找麻煩.
更新至第98集
新還珠格格...
更新至第21集
來自星星的你
電視劇
綜藝
動漫
搜尋
更多
free for personal use


啊
啊

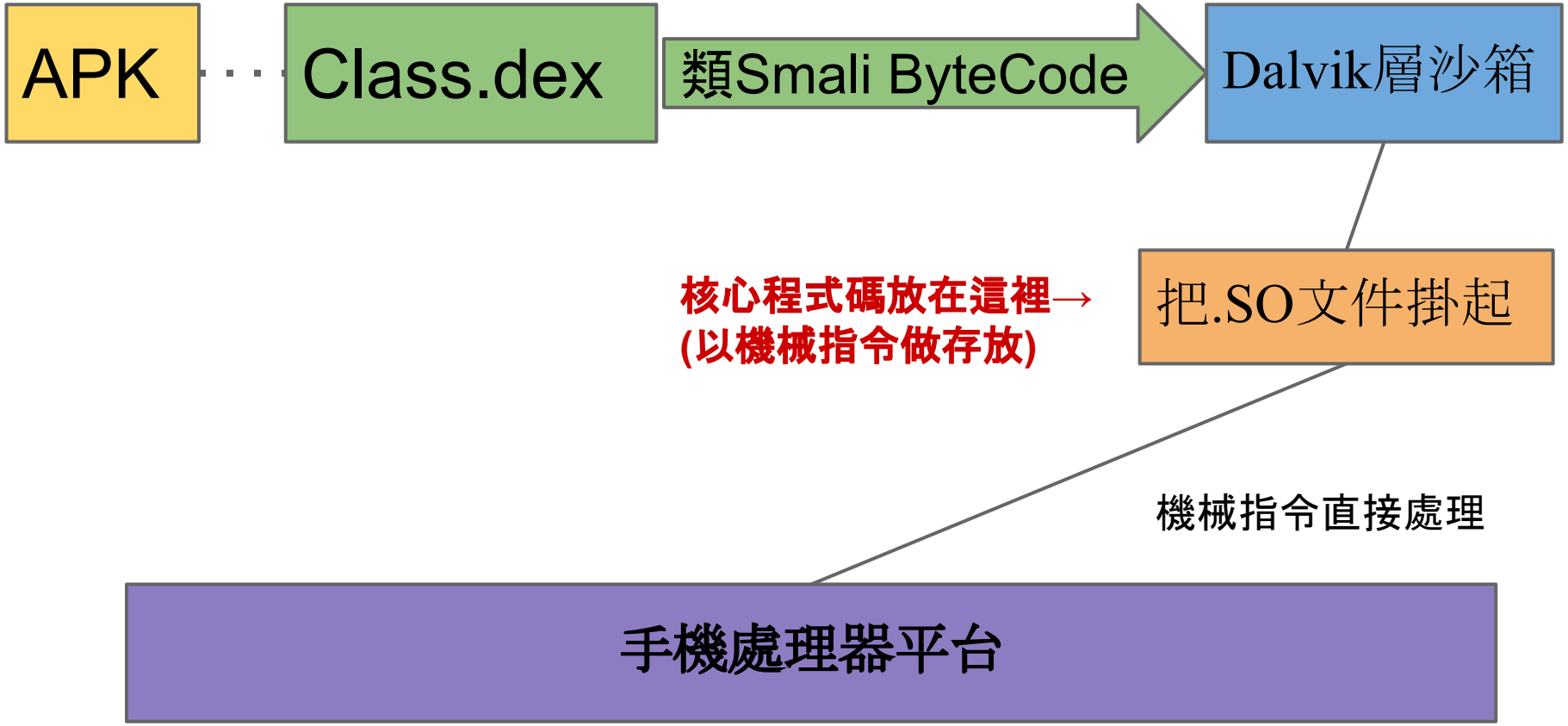
既然APK逆向這麼乾丹

那是否聽完這場我就成為了APK逆向大神？

Android SDK App



Android NDK App




幹你媽這三小

好消息是

因為NDK是近一年才被Google推廣的...所以

目前九成九的市場都是採 Android SDK做開發 (or SDK+.mono)

壞消息是

不是每支App都不加密


你TM在逗我？

But

大部分的加密其實都能功破XD

0x02_額外技能;

我們來談談.NET逆向吧
(((o(*゜▽゜*)o)))

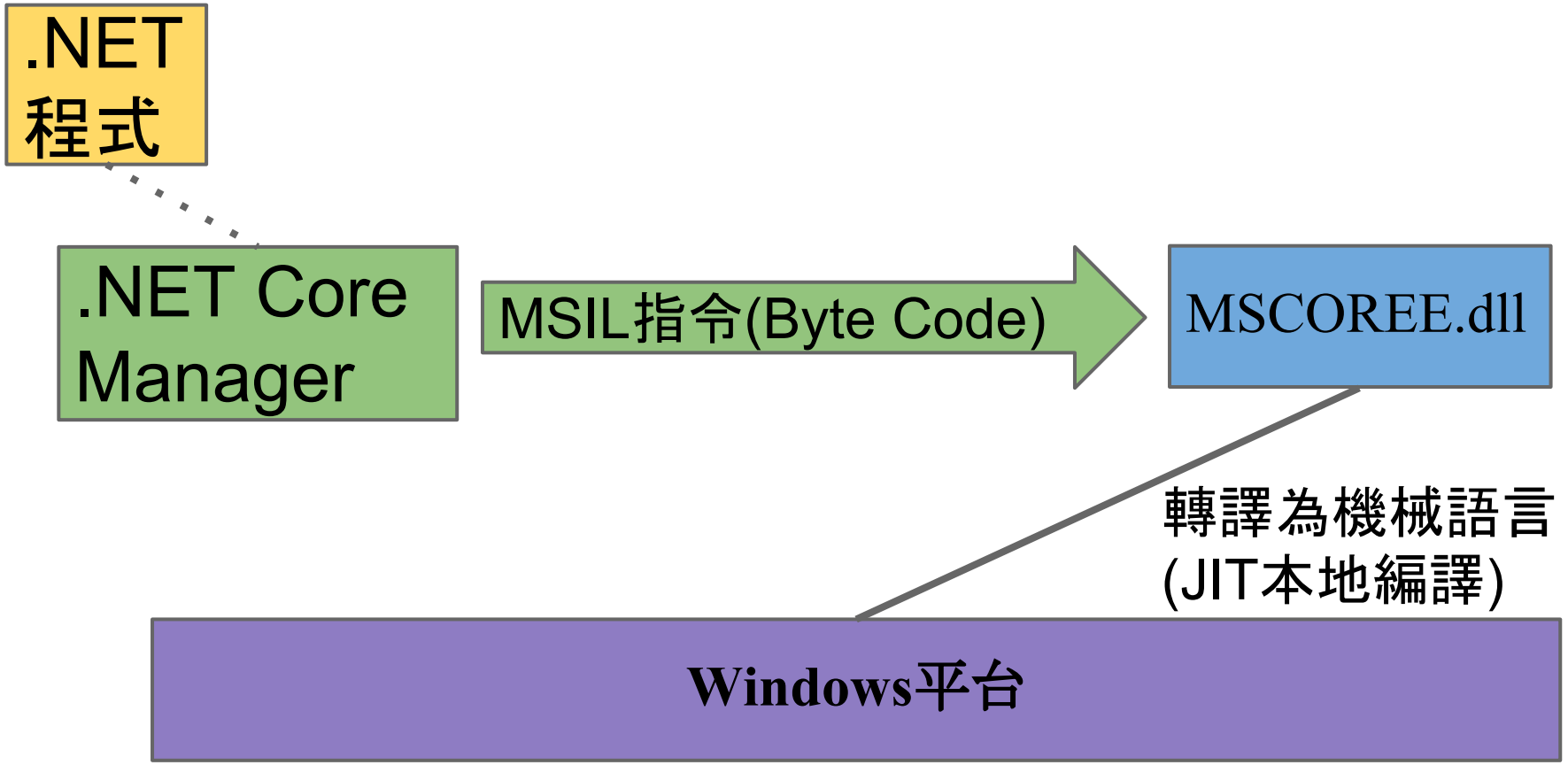
.NET Framework是什麼？

.NET Framework是什麼？

.NET Framework是由微軟開發，一個致力於敏捷軟體開發（Agile software development）、快速應用開發（Rapid application development）、平臺獨立性和網路透明化的軟體開發平臺。.NET是微軟為2000年代對伺服器和桌上型軟體工程邁出的第一步。.NET包含許多有助於網際網路和內部網應用迅捷開發的技術。

喔，字很多不想看嗎XD？

普通的MicroSoft .NET託管程序架構



MicroSoftSIL(CIL其中一類) 連結

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link

Common Intermediate Language

From Wikipedia, the free encyclopedia

For the counterpart to compiled assembly in the Common Language Infrastructure, see assembly (CLI).

Common Intermediate Language (**CIL**, pronounced either "sil" or "kil") (formerly called **Microsoft Intermediate Language** or **MSIL**) is the lowest-level human-readable programming language defined by the Common Language Infrastructure (CLI) specification and is used by the .NET Framework and Mono. Languages which target a CLI-compatible runtime environment compile to CIL, which is assembled into an object code that has a bytecode-style format. CIL is an object-oriented assembly language, and is entirely stack-based. Its bytecode is translated into native code or — most commonly — executed by a virtual machine.

CIL was originally known as Microsoft Intermediate Language (MSIL) during the beta releases of the .NET languages. Due to standardization of C# and the Common Language Infrastructure, the bytecode is now officially known as CIL.[1]

In an independent usage, CIL also refers to the C Intermediate Language, a simplified transformation of C used for further analysis.[2]

Contents [hide]

CIL Byte Code意義 連結

List of CIL instructions

From Wikipedia, the free encyclopedia

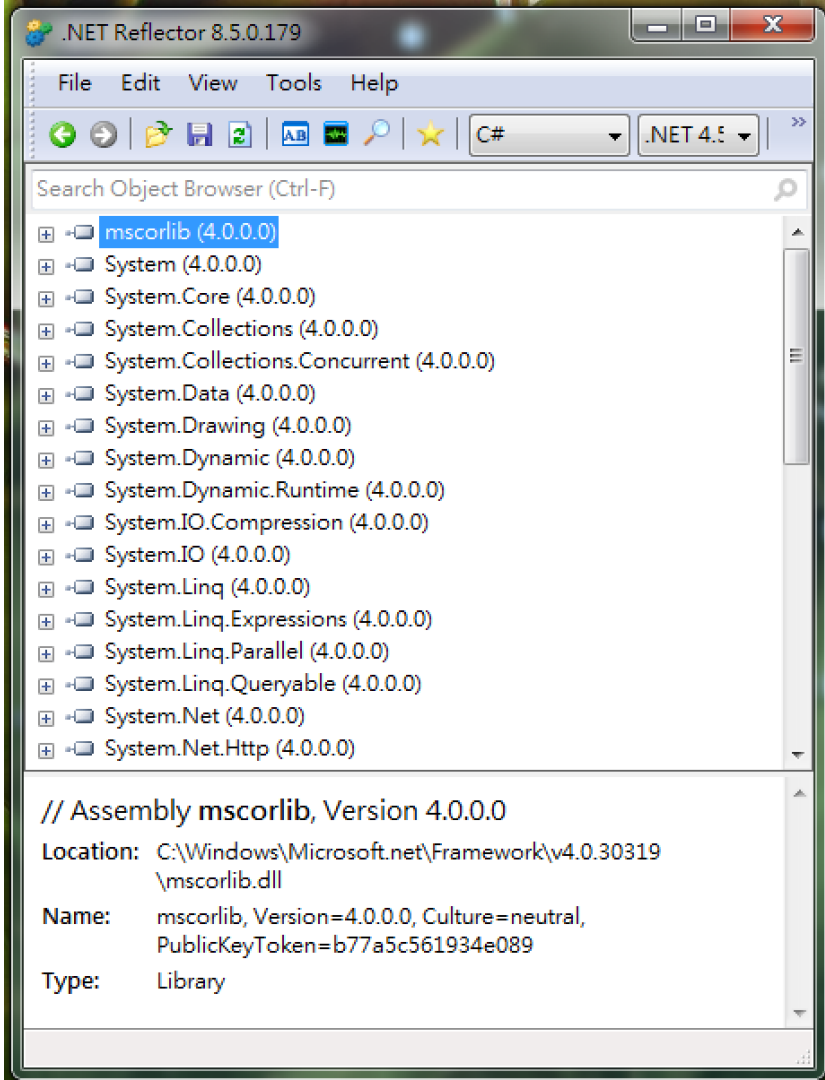
Main article: Common Intermediate Language

This is a list of the instructions in the instruction set of the Common Intermediate Language bytecode.

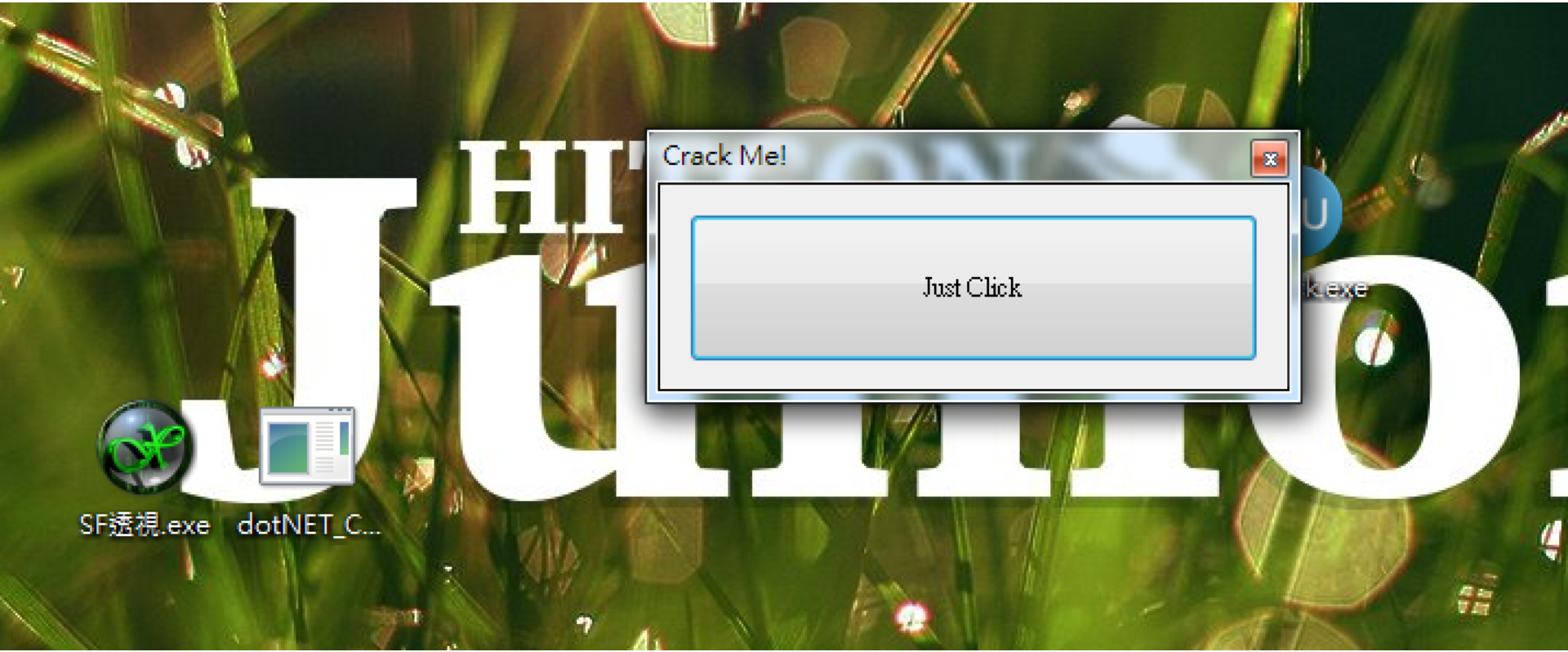
Opcode	Instruction	Description	Type of instruction
0x58	`add`	**Add** two values, returning a new value.	Base instruction
0xD6	`add.ovf`	**Add** signed integer values with **ov**erflow check.	Base instruction
0xD7	`add.ovf.un`	**Add** unsigned integer values with **ov**erflow check.	Base instruction
0x5F	`and`	Bitwise **AND** of two integral values, returns an integral value.	Base instruction

逆向.NET入門包

.NET Reflector 尬 Reflexil Combo組合技



.NET 拆拆練習

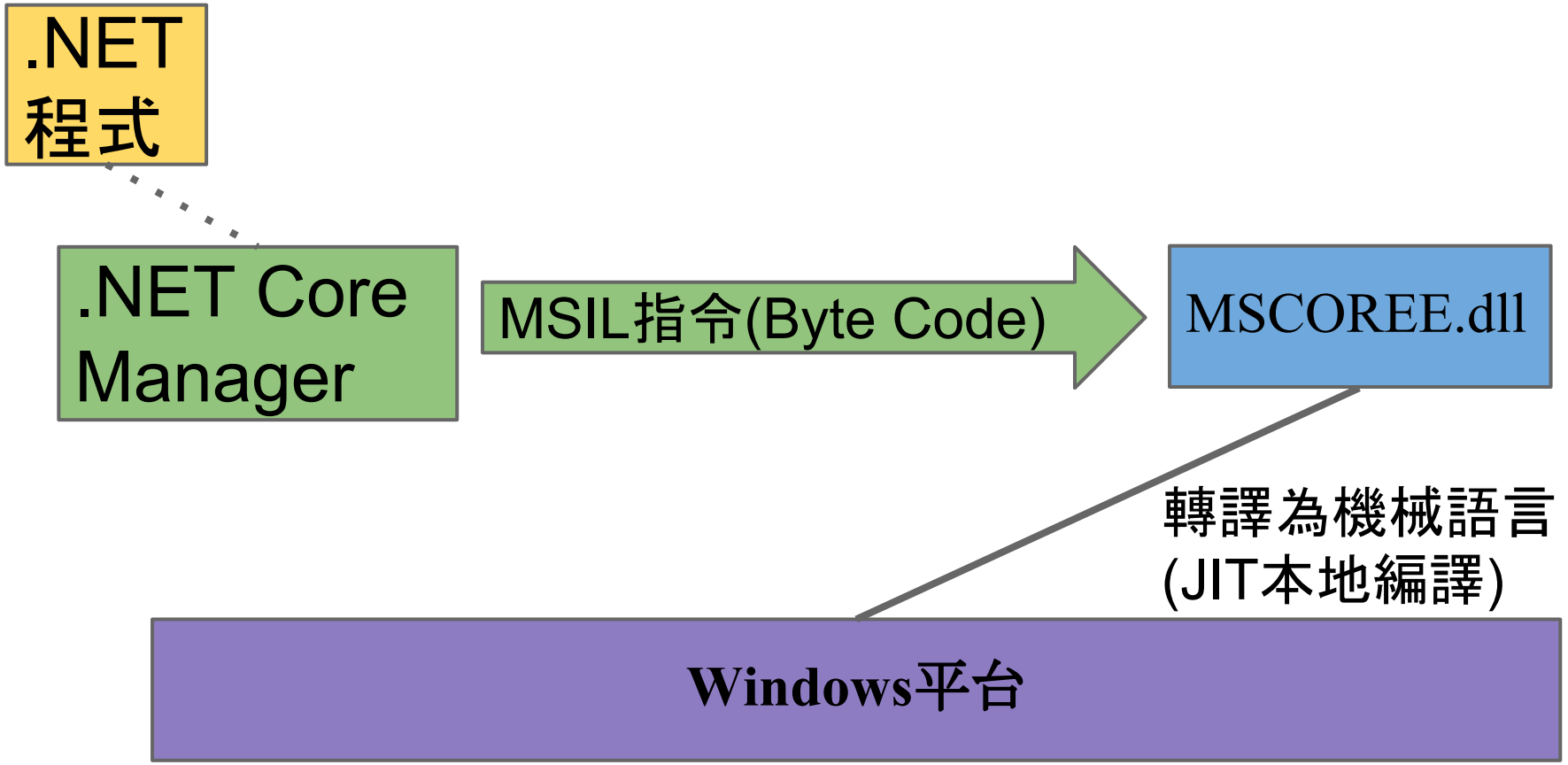


SF商業外掛拆拆實戰！


SF透視.exe
http://sfcheat.4d-host.com/dll/SFWallhack.rar
登入
註冊
儲值
修改密碼
帳號
密碼
登入
獲得機器唯一序號

0x03_Combo;

普通的MicroSoft .NET託管程序架構

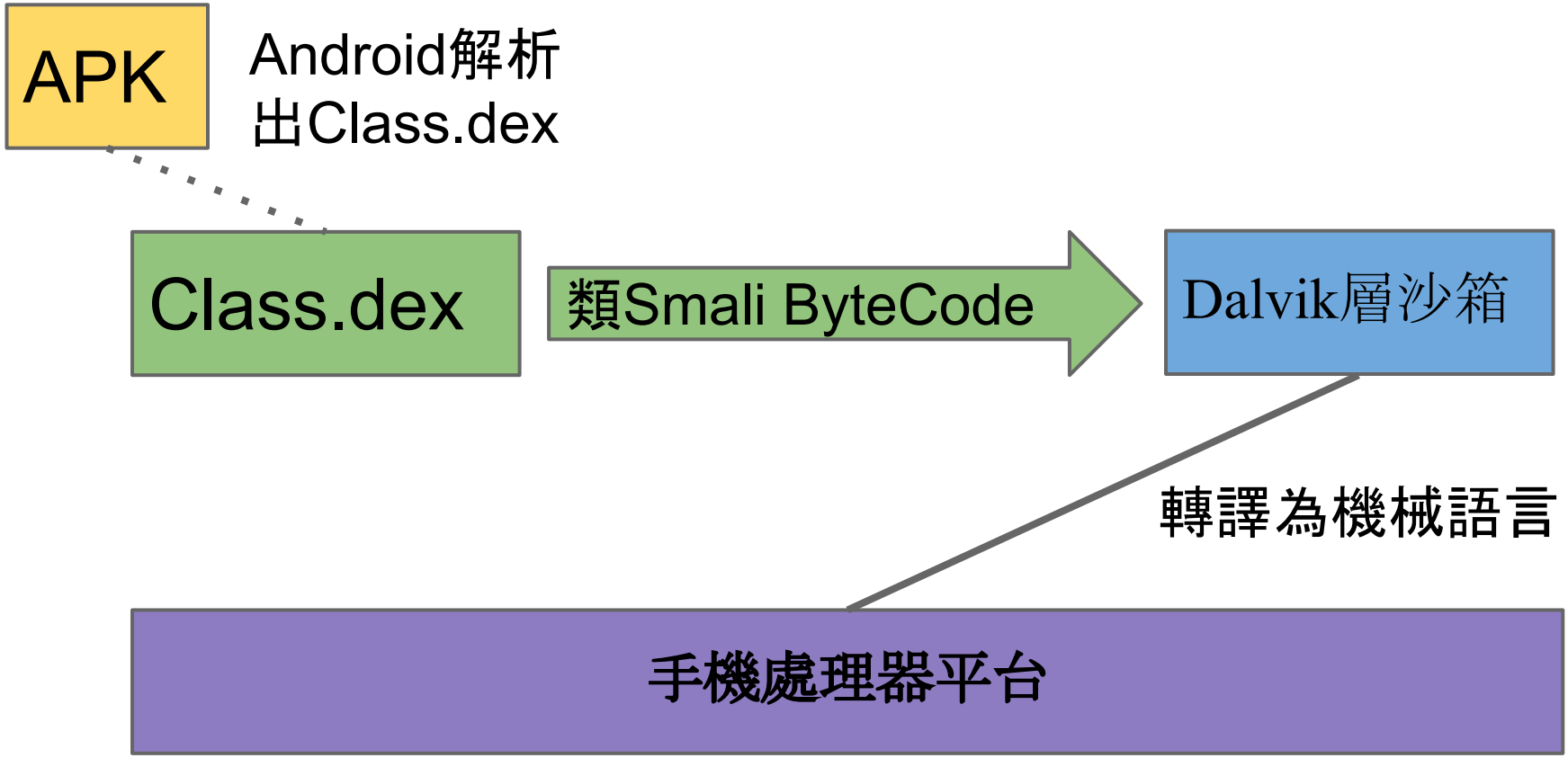


是的，您沒看錯。
Windows Only

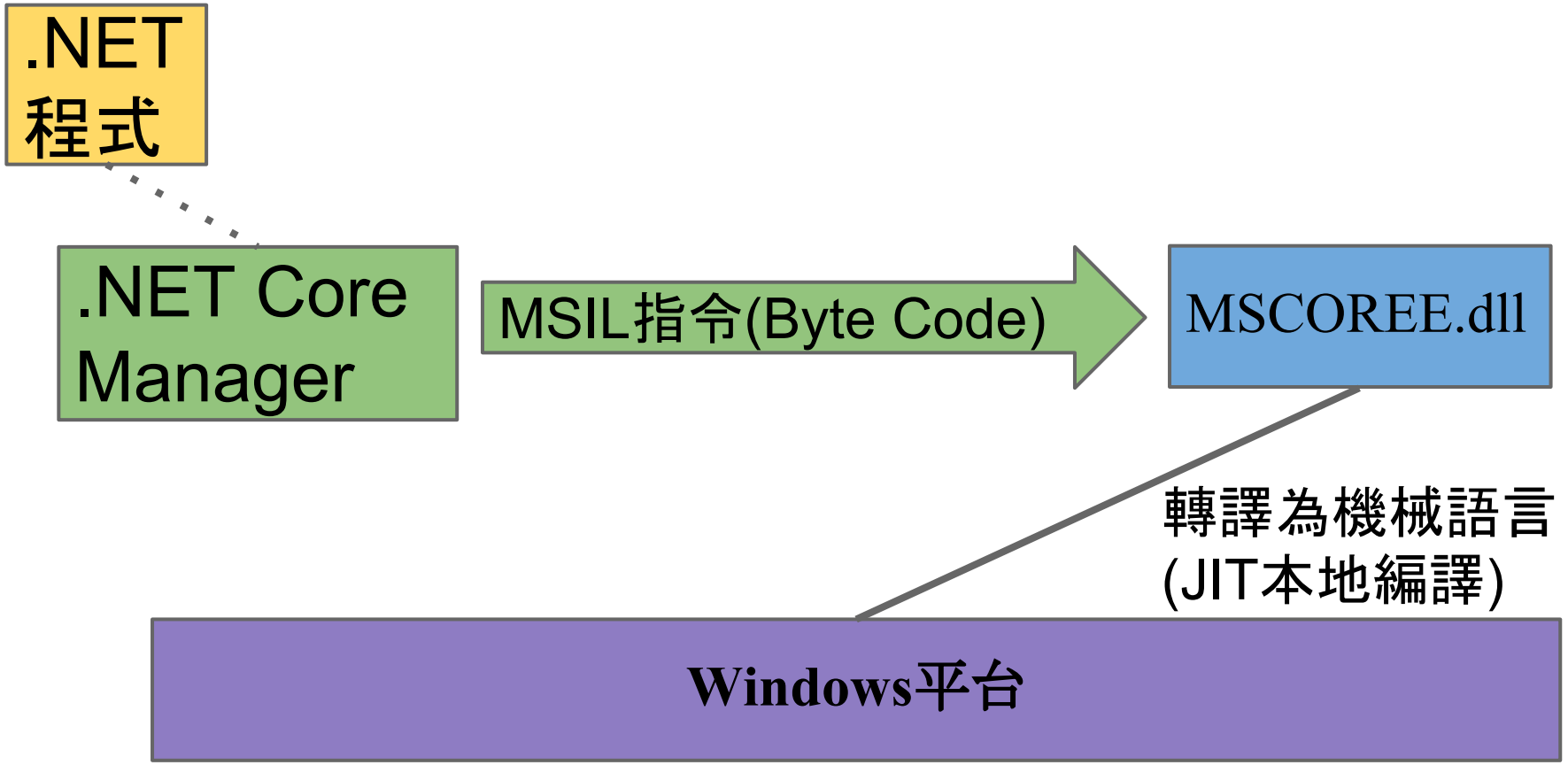

我不能接受

你們一定會想...
那到底幹嘛學這麼廢的東西啊
(゜Д゜)

Android SDK App



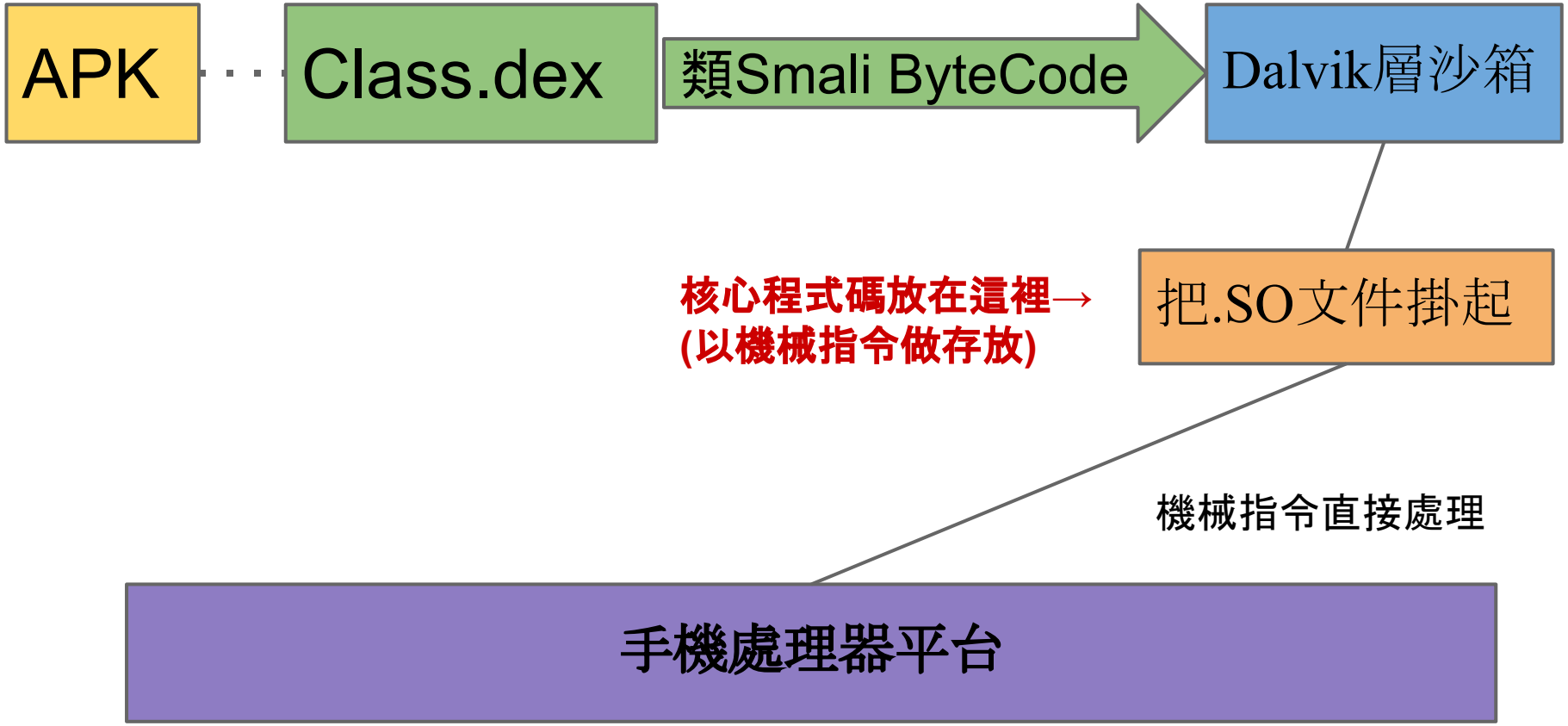
普通的MicroSoft .NET託管程序架構



不覺得真的超像的嗎(゜Д゜)

於是有家公司
Xamarin就想說...

Android NDK App



既然都有TMD
這種噁心的做法

那怎麼沒人做
.NET Framework For U - (Windows Only)

於是MONO這個Open Source的巫術就這樣誕生了

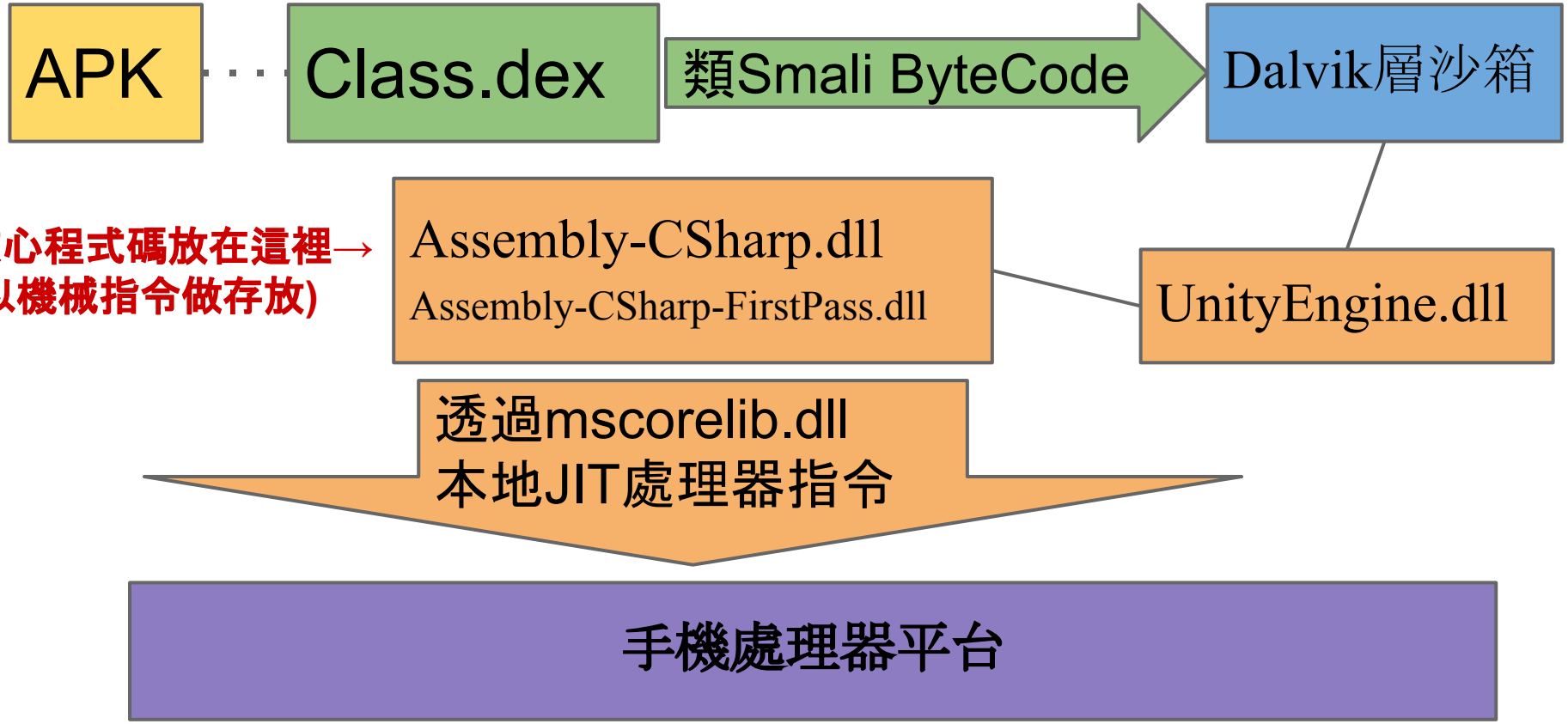
後來MONO專案就被拿去開發手遊引擎 - Unity！

蛤, Unity？
有哪個
手機遊戲用過？


TOILET OF PLAGIARISTS
神抄之塔


TOWER OF SAVIORS
神魔之塔

Unity App架構


APK
Class.dex
類Smali ByteCode
Dalvik層沙箱
核心程式碼放在這裡→
(以機械指令做存放)
Assembly-CSharp.dll
Assembly-CSharp-FirstPass.dll
UnityEngine.dll
透過mscorelib.dll
本地JIT處理器指令
手機處理器平台

那如果我們
今天想對Unity功能動刀？

來自星星的你


違登阿帕契
三立新聞HD
拔掉星星的你
十人共拔二十七顆星
起底百億富豪團
藝人李蒨蓉
台北
有這麼嚴重嗎
12:07:03
三立民調
六都市長滿意度民調 高雄陳菊84.8%奪冠

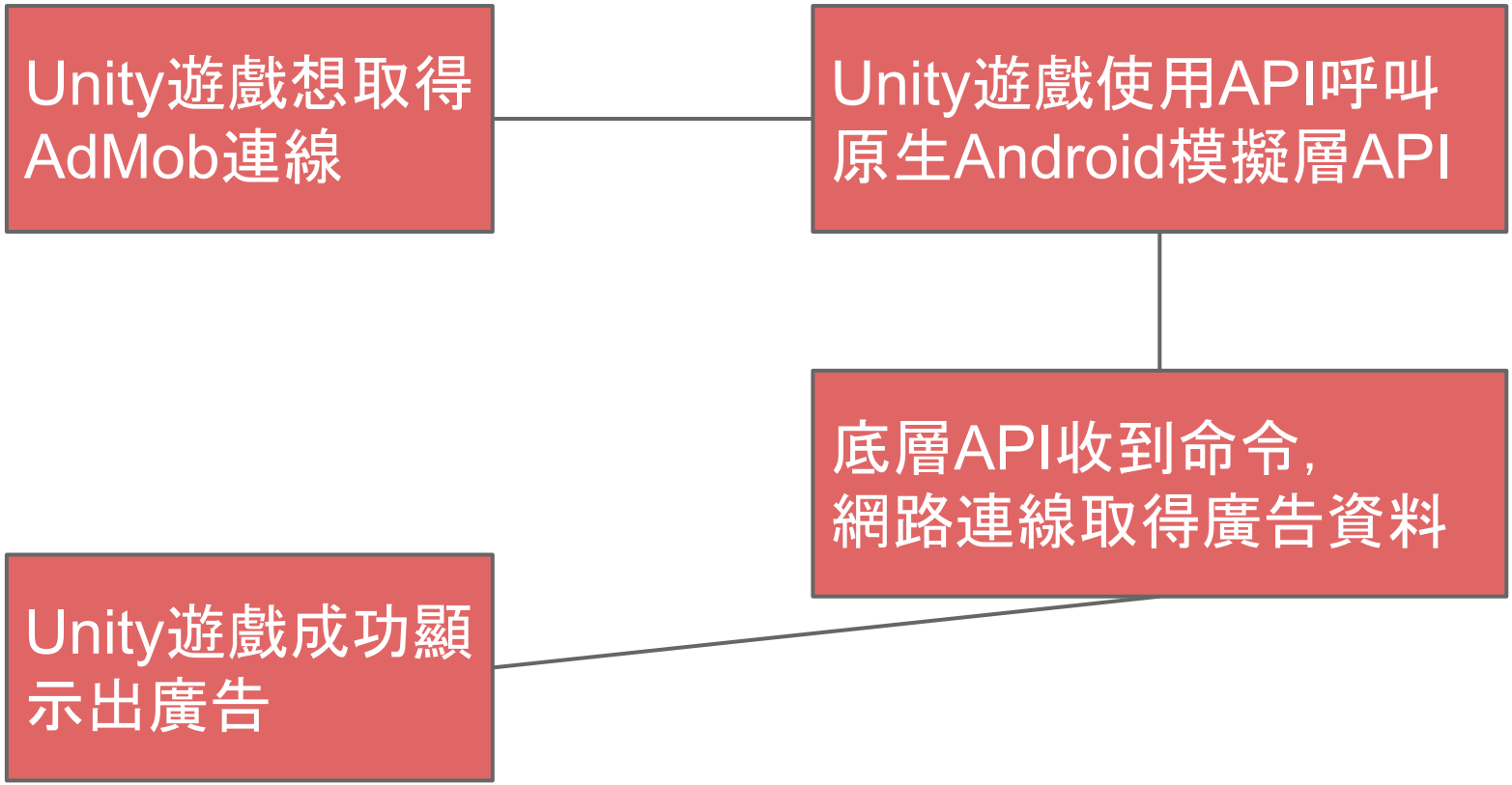

蘋果日報

女星想
和阿帕契拍照

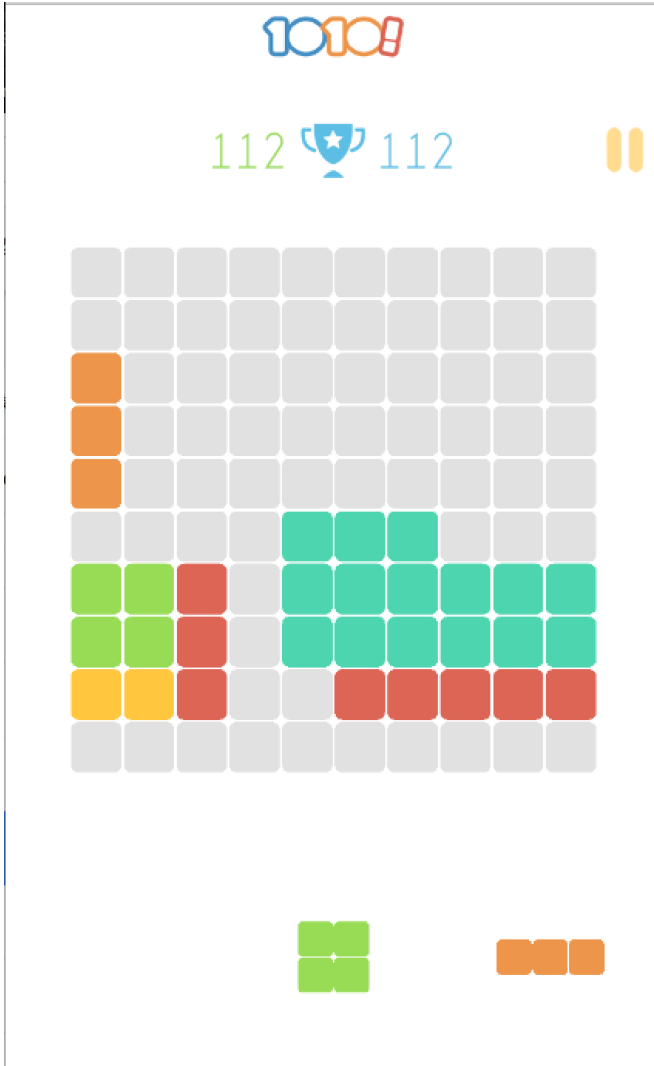
飛官忍住一百萬個小頭癢的
衝動，帶女星進入兵營

檢查小兵不敢阻擋高層
飛官，放行入境

女星成功
和阿帕契拍照


Unity遊戲想取得
AdMob連線
Unity遊戲使用API呼叫
原生Android模擬層API
底層API收到命令,
網路連線取得廣告資料
Unity遊戲成功顯
示出廣告

實戰Google Play上
破百萬熱門小遊戲去廣告
（Unity Engine Game）



我絕對不會說.....

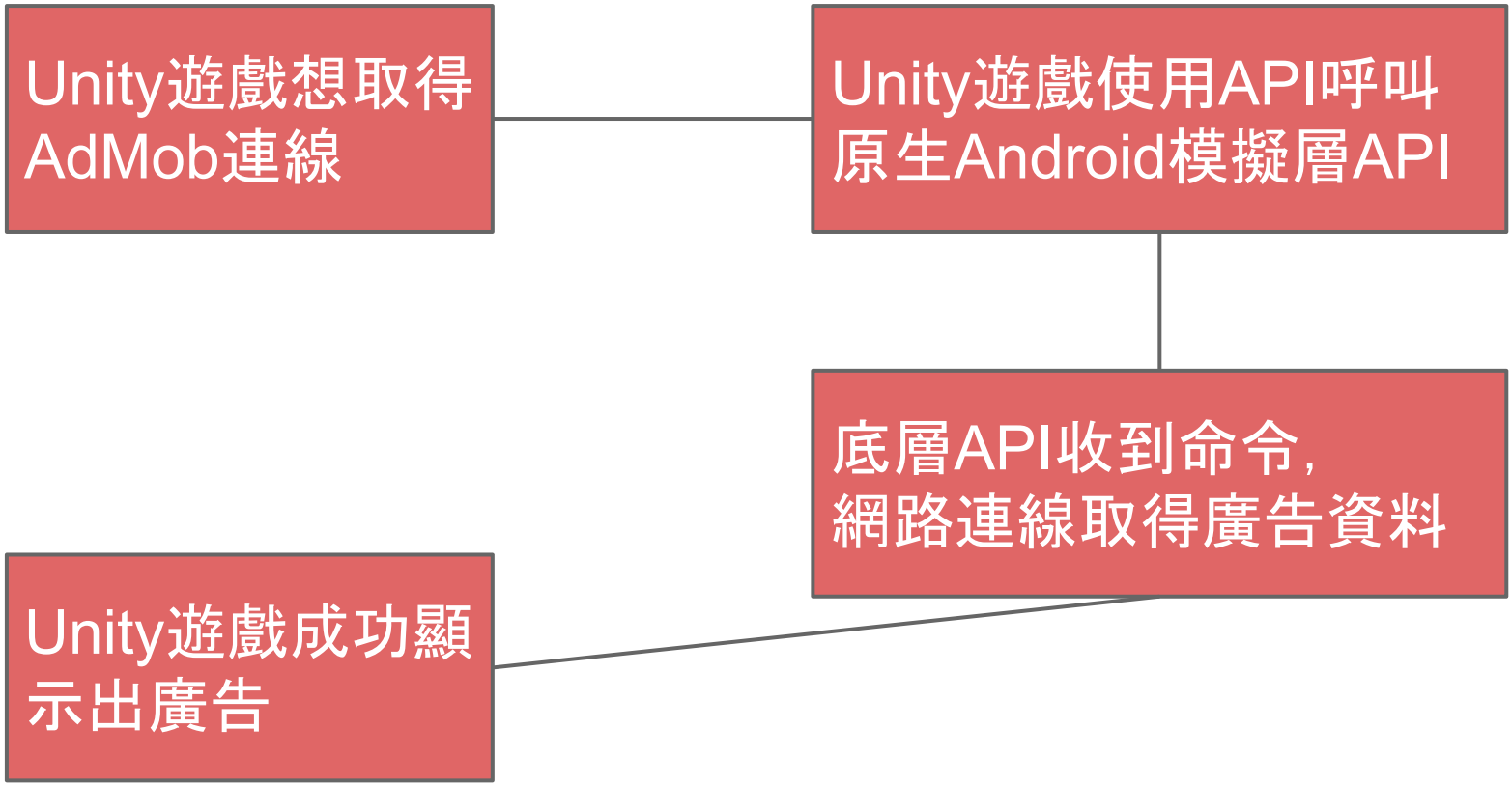
神抄(冂ㄒ´)之塔也是可如法炮製破解打補丁APK der ε-(´∀`;)

女星想
和阿帕契拍照

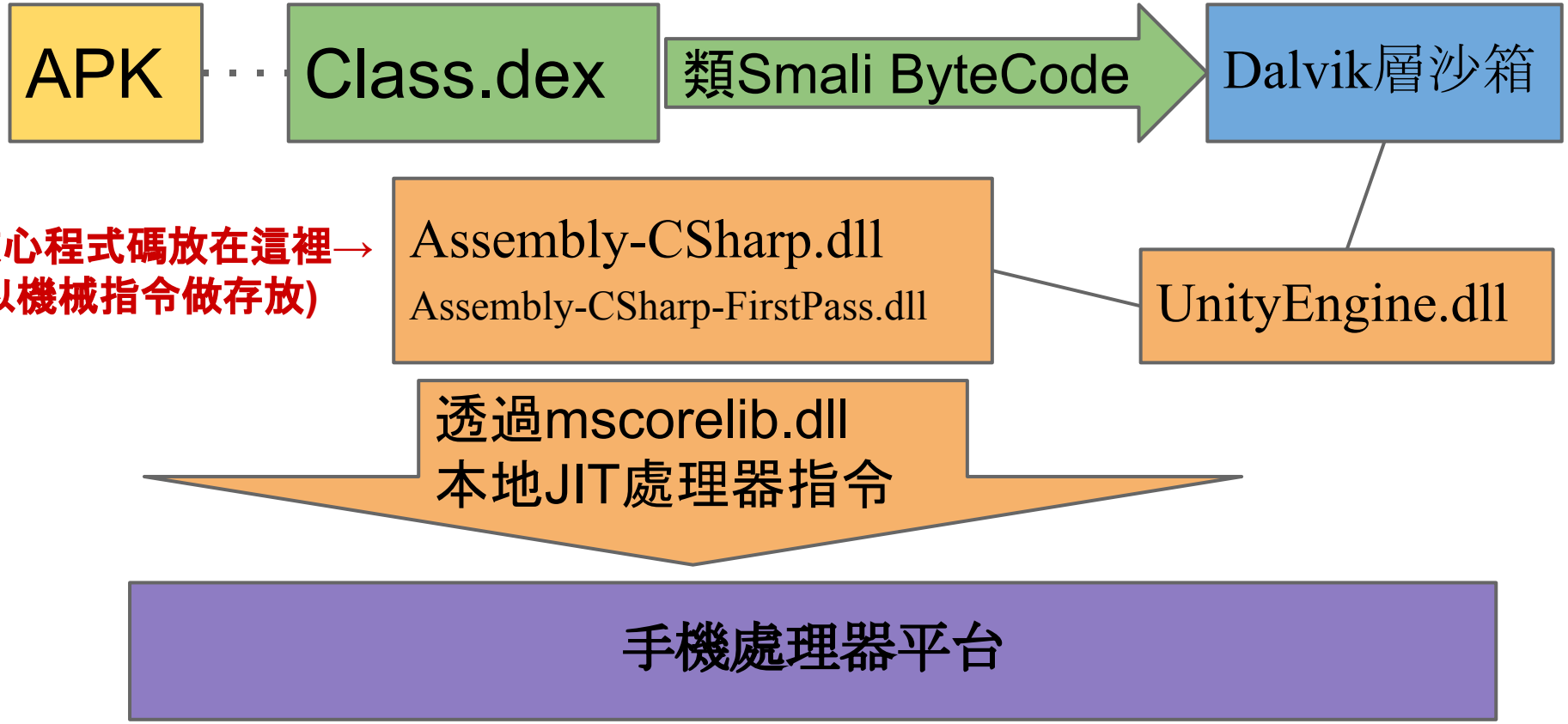
飛官忍住一百萬個小頭癢的
衝動，帶女星進入兵營

檢查小兵不敢阻擋高層
飛官，放行入境

女星成功
和阿帕契拍照


Unity遊戲想取得
AdMob連線
Unity遊戲使用API呼叫
原生Android模擬層API
底層API收到命令,
網路連線取得廣告資料
Unity遊戲成功顯
示出廣告

Unity App架構


APK
Class.dex
類Smali ByteCode
Dalvik層沙箱
核心程式碼放在這裡→
(以機械指令做存放)
Assembly-CSharp.dll
Assembly-CSharp-FirstPass.dll
UnityEngine.dll
透過mscorelib.dll
本地JIT處理器指令
手機處理器平台

DEMO

馬聖豪(ADR)

Q&A Time.

helloadr.blogspot.tw

aaaddress1@gmail.com