# *Hack Mobile Games For Fun*


***HITCON 2015***

***ChienWei Hung (winest)***


***2015/08/29***

- 四年前~~被騙~~入趨勢當研替
- 遊戲資歷22年
  - 永遠的β測試玩家


BONUSTIME
277
834,418
下個目標
第1名
3025203
Jump
Slide
YOUR TURN!
關閉
Lv. 20 烨練弓箭手
Pass
Backpack


所以你到底是來幹嘛的？

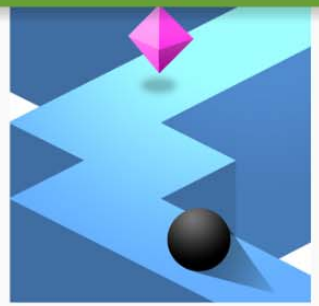
# 來聊聊手機遊戲破解

CATEGORIES HOME TOP PAID TOP FREE TOP GROSSING TOP NEW PAID TOP NEW FREE

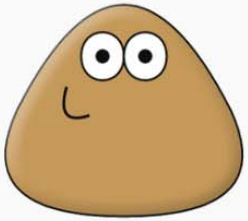
69. LEGO® Ninjago
The LEGO Group
★★★★½ FREE

70. Gangstar Vegas
Gameloft
★★★★½ FREE

71. DH Texas Poker - Texas
DroidHen
★★★★½ FREE



72. ZigZag
Ketchapp
★★★★½ FREE

# 2014年營收

| Rank | iOS App Store |
|---|---|
| 10 | **Taiwan** |
| 9 | Russia |
| 8 | France |
| 7 | Germany |
| 6 | Canada |
| 5 | Australia |
| 4 | United Kingdom |
| 3 | China |
| 2 | Japan |
| 1 | United States |

| Rank | Google Play |
|---|---|
| 1 | Japan |
| 2 | United States |
| 3 | South Korea |
| 4 | Germany |
| 5 | **Taiwan** |
| 6 | United Kingdom |
| 7 | France |
| 8 | Hong Kong |
| 9 | Australia |
| 10 | Canada |

from App Annie

# LV. 0

Google 破解 解鎖 已付費

[redacted]平台

標題: 求殭屍戰爭漢化破解版

---

作者:[redacted] 時間: **2015-6-11 10:43**
標題: 求殭屍戰爭漢化破解版
在別的網站上有免驗證的殭屍戰爭漢化版，希望破解金幣不然窮，謝謝！

---

作者:[redacted]時間: **2015-6-11 14:25**
這個遊戲貌似很久沒更新了，大神可能不破解的

---

作者:[redacted] 時間: **2015-7-2 13:26**
好帖，確實好帖！

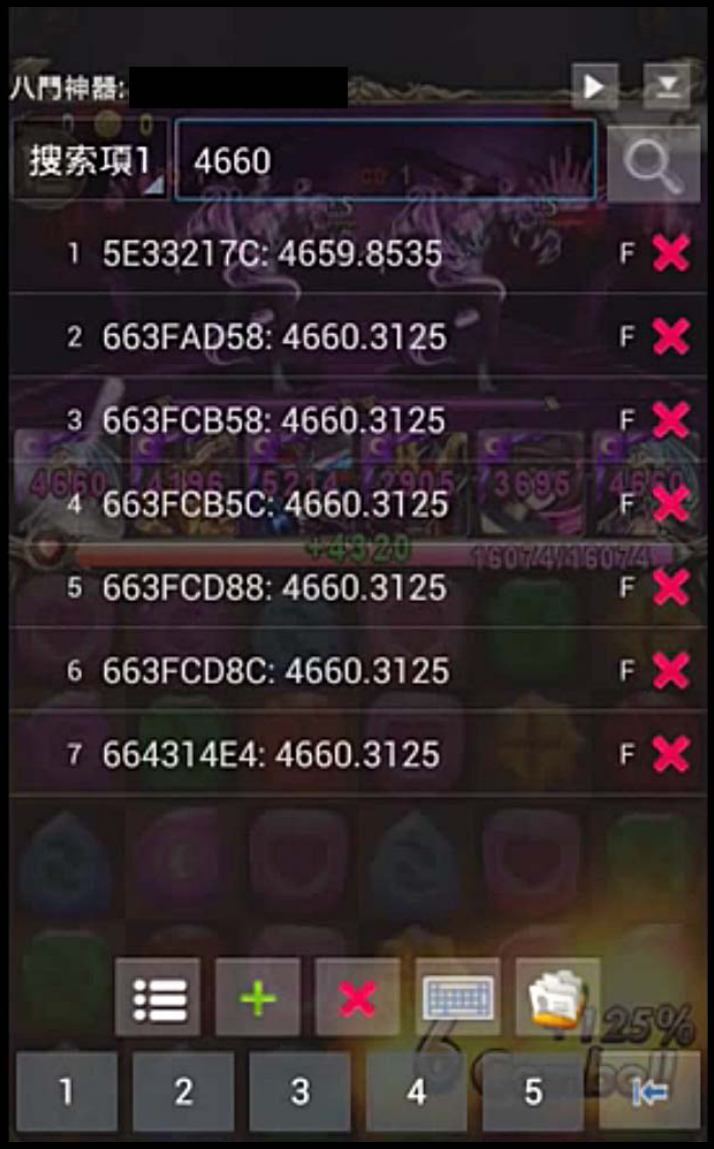
---

作者:[redacted] 時間: **2015-7-4 17:46**
確實值得好好看看，頂先

---

作者:[redacted]時間: **2015-7-20 04:20**
**LZ辛苦了，支持一下！**

# LV. 1


八門神器:
搜索項1
4660
1 5E33217C: 4659.8535 F
2 663FAD58: 4660.3125 F
3 663FCB58: 4660.3125 F
4 663FCB5C: 4660.3125 F
5 663FCD88: 4660.3125 F
6 663FCD8C: 4660.3125 F
7 664314E4: 4660.3125 F
1
2
3
4
5

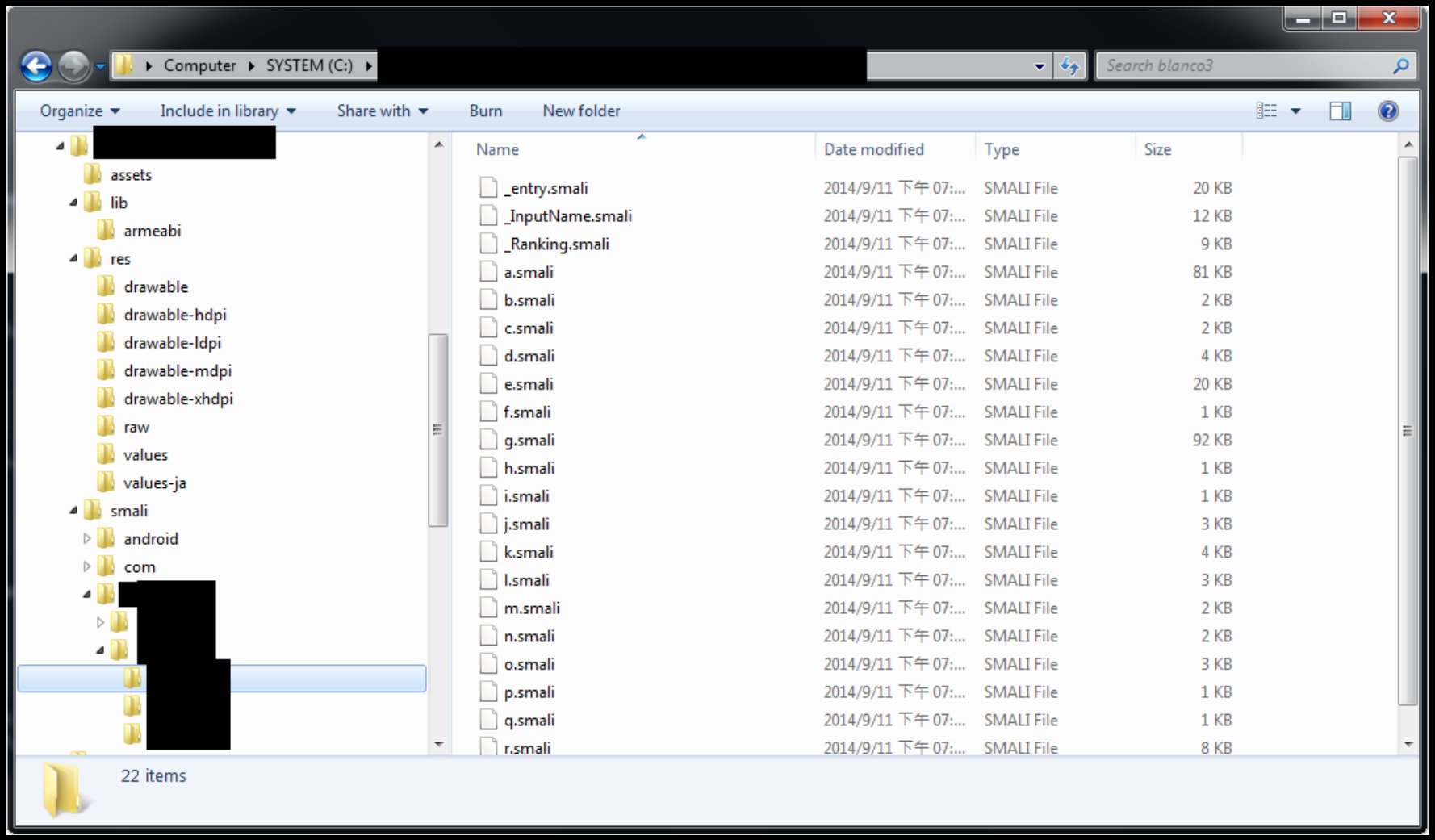

+2166
9300/16074
2 Combo!!
+25%

# LV. 1 限制

- Root
- Memory未加密
- 程式的驗證很弱
  - Root檢查
  - 已安裝程式檢查
  - 動作前後數值檢查

# LV. 2

- Unpack apk
  - java -jar apktool.jar d -f “<src apk>” -o “<dst folder>”
- Repack apk
  - java -jar apktool.jar b “<dst folder>”
  - java -jar signapk.jar “<pem file>” “<pk8 file>” “<unsigned apk>” “<signed apk>”

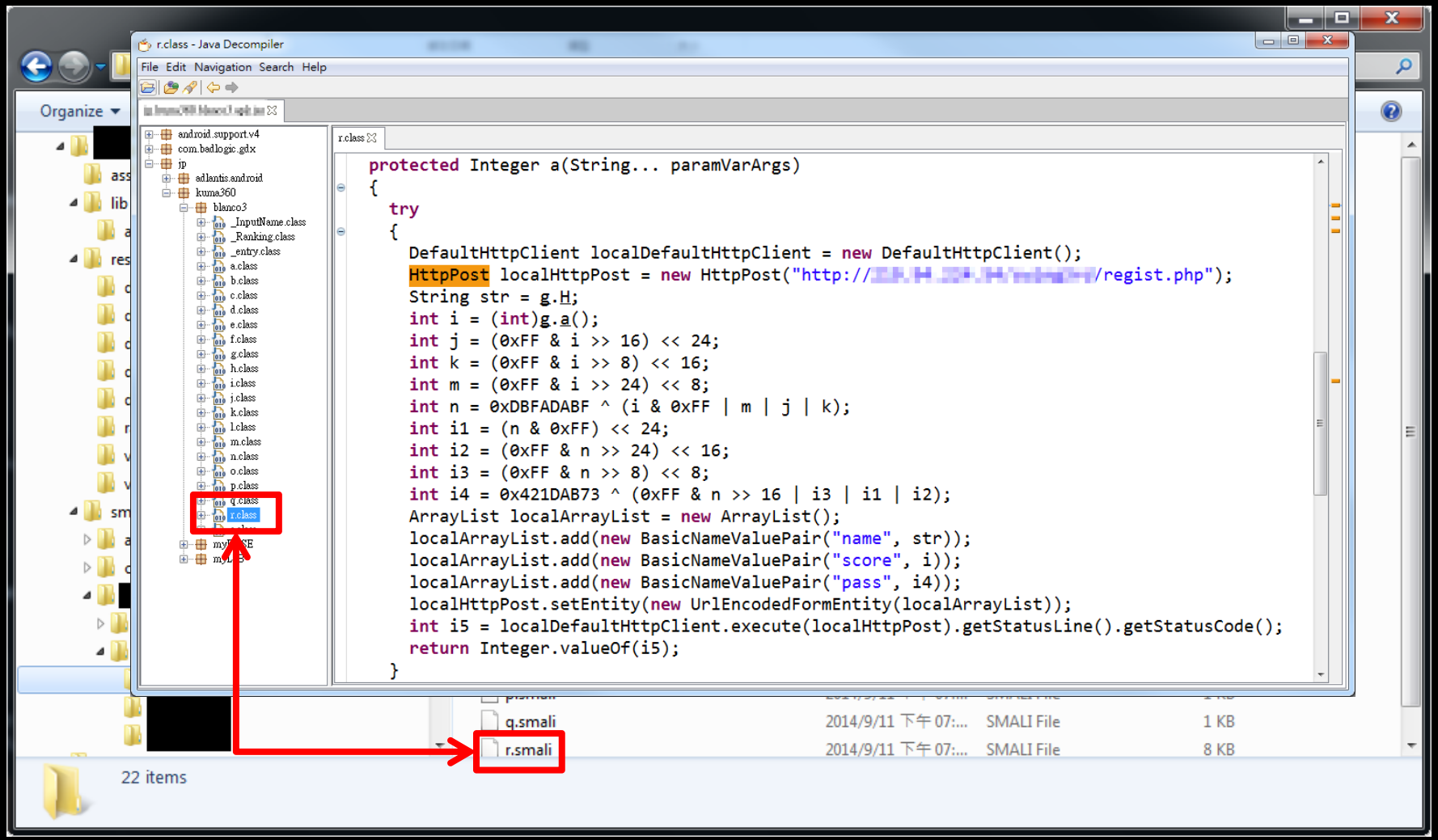

Computer ▸ SYSTEM (C:) ▸
Search blanco3
Organize
Include in library
Share with
Burn
New folder
[redacted]
assets
lib
armeabi
res
drawable
drawable-hdpi
drawable-ldpi
drawable-mdpi
drawable-xhdpi
raw
values
values-ja
smali
android
com
[redacted]
Name
Date modified
Type
Size
_entry.smali 2014/9/11 下午 07:... SMALI File 20 KB
_InputName.smali 2014/9/11 下午 07:... SMALI File 12 KB
_Ranking.smali 2014/9/11 下午 07:... SMALI File 9 KB
a.smali 2014/9/11 下午 07:... SMALI File 81 KB
b.smali 2014/9/11 下午 07:... SMALI File 2 KB
c.smali 2014/9/11 下午 07:... SMALI File 2 KB
d.smali 2014/9/11 下午 07:... SMALI File 4 KB
e.smali 2014/9/11 下午 07:... SMALI File 20 KB
f.smali 2014/9/11 下午 07:... SMALI File 1 KB
g.smali 2014/9/11 下午 07:... SMALI File 92 KB
h.smali 2014/9/11 下午 07:... SMALI File 1 KB
i.smali 2014/9/11 下午 07:... SMALI File 1 KB
j.smali 2014/9/11 下午 07:... SMALI File 3 KB
k.smali 2014/9/11 下午 07:... SMALI File 4 KB
l.smali 2014/9/11 下午 07:... SMALI File 3 KB
m.smali 2014/9/11 下午 07:... SMALI File 2 KB
n.smali 2014/9/11 下午 07:... SMALI File 2 KB
o.smali 2014/9/11 下午 07:... SMALI File 3 KB
p.smali 2014/9/11 下午 07:... SMALI File 1 KB
q.smali 2014/9/11 下午 07:... SMALI File 1 KB
r.smali 2014/9/11 下午 07:... SMALI File 8 KB
22 items

r.smali

```
142     new-instance v0, Lorg/apache/http/message/BasicNameValuePair;
143
144     const-string v6, "score"
145
146     new-instance v7, Ljava/lang/StringBuilder;
147
148     invoke-direct {v7}, Ljava/lang/StringBuilder;-><init>()V
149
150     invoke-virtual {v7, v3}, Ljava/lang/StringBuilder;->append(I)Ljava/lang/StringBuilder;
151
152     move-result-object v3
153
154     invoke-virtual {v3}, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
155
156     move-result-object v3
157
158     invoke-direct {v0, v6, v3}, Lorg/apache/http/me                                    String;)V
159
160     invoke-interface {v5, v0}, Ljava/util/List;->ad
161
162     new-instance v0, Lorg/apache/http/message/Basic
163
164     const-string v3, "pass"
165
166     new-instance v6, Ljava/lang/StringBuilder;
167
168     invoke-direct {v6}, Ljava/lang/StringBuilder;->
169
170     invoke-virtual {v6, v4}, Ljava/lang/StringBuild
171
172     move-result-object v4
173
174     invoke-virtual {v4}, Ljava/lang/StringBuilder;->toString()Ljava/lang/String;
175
176     move-result-object v4
```

# Bytecode的好處

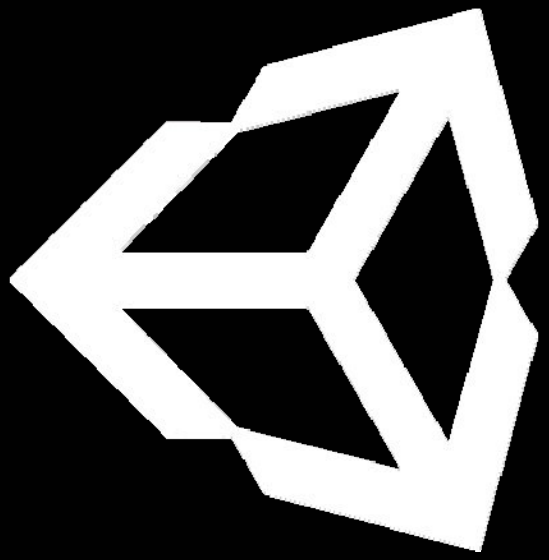
- 可以直接看source code
  - d2j-dex2jar -f “<src apk>” -o “<dst jar>”
  - jd-gui “<dst jar>”


r.class - Java Decompiler
File Edit Navigation Search Help
android.support.v4
com.badlogic.gdx
jp
adlantis.android
kuma360
blanco3
_InputName.class
_Ranking.class
_entry.class
a.class
b.class
c.class
d.class
e.class
f.class
g.class
h.class
i.class
j.class
k.class
l.class
m.class
n.class
o.class
p.class
q.class
r.class
r.class
protected Integer a(String... paramVarArgs)
{
try
{
DefaultHttpClient localDefaultHttpClient = new DefaultHttpClient();
HttpPost localHttpPost = new HttpPost("http://[redacted]/regist.php");
String str = g.H;
int i = (int)g.a();
int j = (0xFF & i >> 16) << 24;
int k = (0xFF & i >> 8) << 16;
int m = (0xFF & i >> 24) << 8;
int n = 0xDBFADABF ^ (i & 0xFF | m | j | k);
int i1 = (n & 0xFF) << 24;
int i2 = (0xFF & n >> 24) << 16;
int i3 = (0xFF & n >> 8) << 8;
int i4 = 0x421DAB73 ^ (0xFF & n >> 16 | i3 | i1 | i2);
ArrayList localArrayList = new ArrayList();
localArrayList.add(new BasicNameValuePair("name", str));
localArrayList.add(new BasicNameValuePair("score", i));
localArrayList.add(new BasicNameValuePair("pass", i4));
localHttpPost.setEntity(new UrlEncodedFormEntity(localArrayList));
int i5 = localDefaultHttpClient.execute(localHttpPost).getStatusLine().getStatusCode();
return Integer.valueOf(i5);
}
Organize
q.smali
2014/9/11 下午 07:... SMALI File 1 KB
r.smali
2014/9/11 下午 07:... SMALI File 8 KB
22 items

# LV. 2 限制

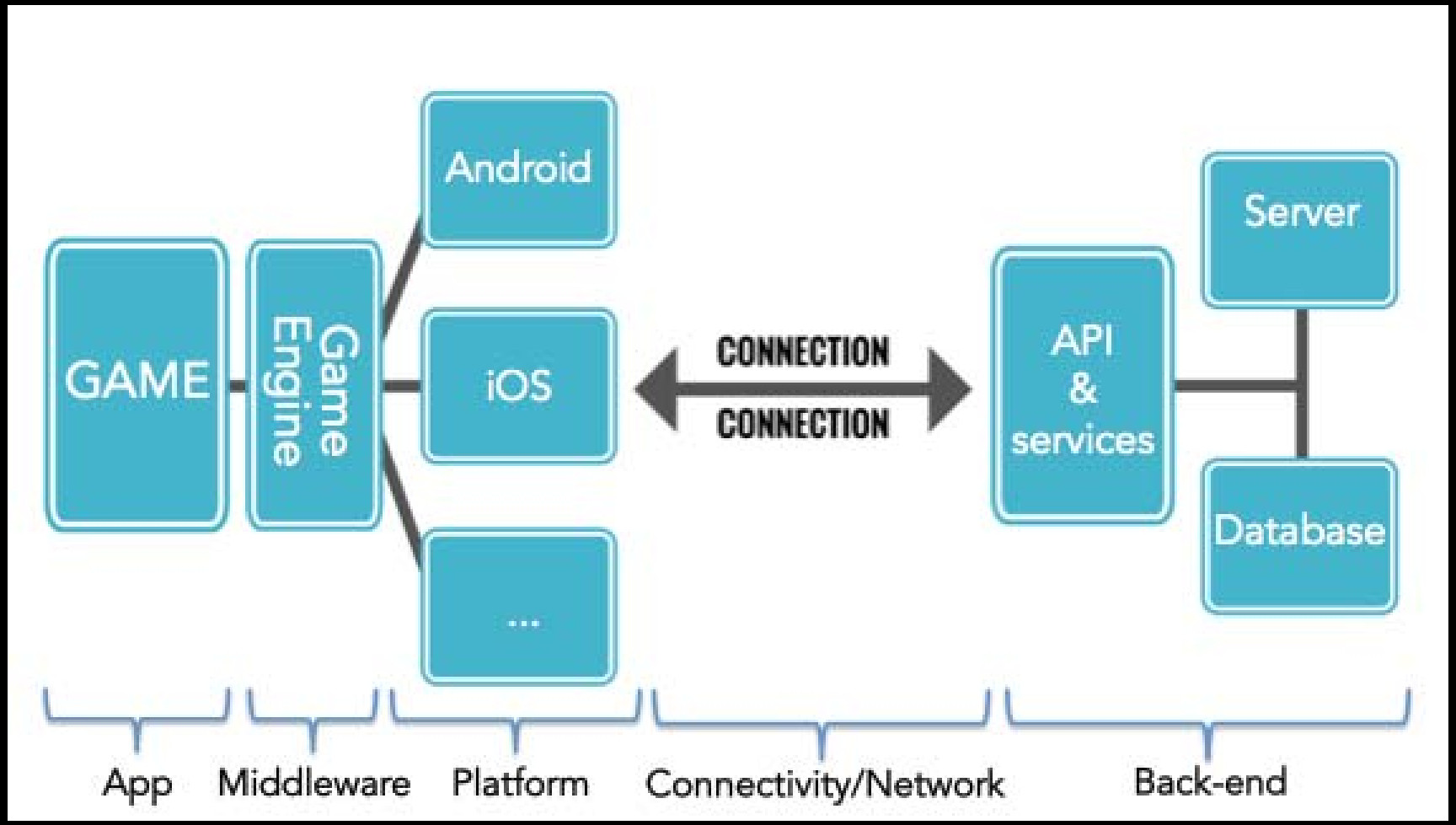
- 沒有被obfuscated
- 程式沒有檢查checksum
- 主程式用Java寫

LV. 3



unity

# 手機遊戲架構

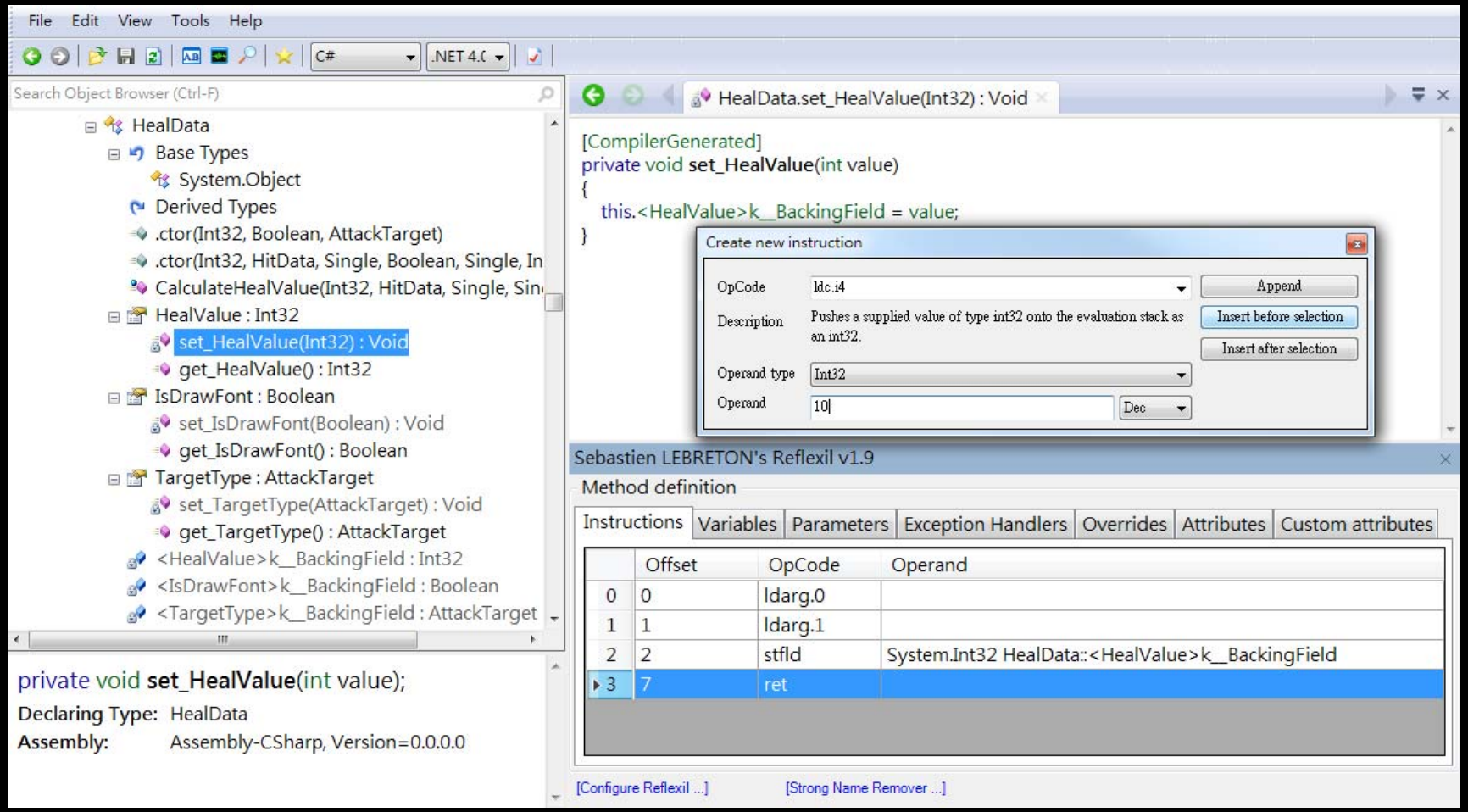

Android
GAME
Game Engine
iOS
...
CONNECTION
CONNECTION
API & services
Server
Database
App
Middleware
Platform
Connectivity/Network
Back-end

# 簡易數值修改

- Unpack apk
- Disassemble到il
  - ildasm.exe <dll path> /OUT=<il path> /UTF8
- 修改*.il
- Assemble回dll
  - ilasm.exe <il path> /DLL /OUTPUT=<dll path> /RESOURCE=<res path>
- Repack and sign apk

# LV. 4

- .NET Reflector配合Reflexil



# LV. 5

- Visual Studio客製化修改
- 自 製Tool調整offset
  - https://github.com/winest/CILTools

# 防禦

- Obfuscate
  - Android有，Unity也有，就是沒人用，超爽der
- 內容加密
- 合理範圍檢查
- 適可而止，否則兩敗俱傷 XD

兩敗俱傷 XD

兩敗俱傷 XD

# 大家來研究

- 如果你符合
  - 我講的你都會了
  - 各式Game Engine或iOS專家
  - 願意提供1G RAM以上iOS機種做研究
- 歡迎來聊聊不一樣的東東

# Q&A

# *Thanks ^ ^*

本人在此特地聲明：
本人樂觀開朗，身體健康，無任何使我困擾之慢性病或心理疾病，故絕不可能做出任何看似自殺之行為。
本人從無睡眠困擾，故不需服用安眠藥。本人不酗酒亦不吸毒，也絕不會接近下列地點—
1. 開放性水域　2. 無救生員之遊泳池　3. 有高壓、危險氣體，或密閉式未經抽氣處理之地下室、蓄水池、水桶等
4. 無安全護欄之任何高處　5. 任何施工地點（拆政府除外），包括製作消波塊之工地
6. 任何以上未提及但為一般人正常不會前往之地點
本人恪遵下列事項—
1. 車輛上路前會檢查煞車部件、油門線等，並會在加油前關閉車輛電源與行動電話。
2. 絕不擅搶黃燈、闖紅燈。　3. 乘坐任何軌道類交通工具一定退到警戒線後一步以上，直到車輛停妥。
4. 騎乘機車必戴安全帽；乘車必繫安全帶。　5. 絕不接近任何會放射對人體有立即危害的輻射之場所或設備。
6. 颱風天不登山、不觀浪、不泛舟。
本人將儘可能注意電器、瓦斯、火源、水源之使用。
本人居住之房屋均使用符合法規之電路電線，絕無電線走火之可能；也絕未在家中放置過量可燃性氣體或液體。
浴室中除該有之照明外，不放置任何電器用品，並在睡覺前關閉除電燈、冰箱、電扇外之所有電器開關。
本人絕不會與隨機的不明人士起衝突，並儘可能保護自我人身安全。
所以若各位在看完此聲明之後，近期或將來發現本人不再上線，請幫我討回公道，謝謝。