- Thxer.com -

Les Articles |\|on-Geek By Thxer For Commu N-PN

Intro Reverse et Patch Android (.apk)

Aujourd'hui débutons le reverse sous Android, ou plutôt des .apk

Les outils :
Sur le Labo

Le SDK android :
https://developer.android.com/sdk/index.html#download

JRE 1.7 :
http://www.oracle.com/technetwork/java/javase/downloads/java-se-jre-7-download-432155.html

Autosign_Apk :
http://dl.dropbox.com/u/9377433/frandroid/autosign.zip

BackSmali & Smali :
https://code.google.com/p/smali/
(Desassembleur / Assembleur de .dex)

Sur l'appreil Android

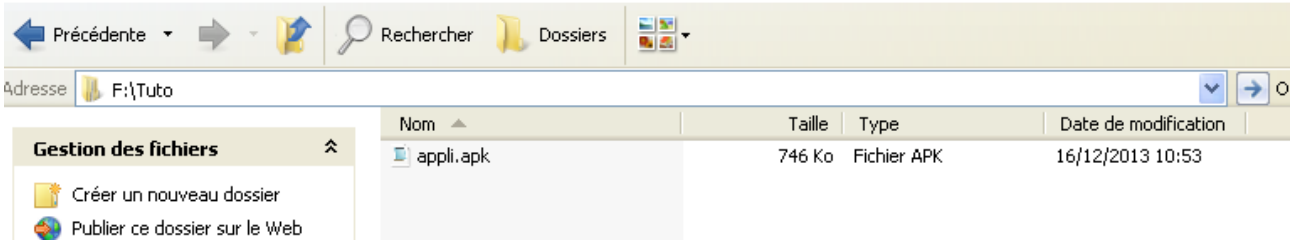
Activer l'installation des applications hors Google Play
Es Explorateur (Appli) / Appli
AppMonster Free (pour recup les .apk) / Appli

PHASE 1 : Récupération d'un .APK

Rien d'extraordinaire lancer : App Monster, sélectionner une Appli , « Backup ».

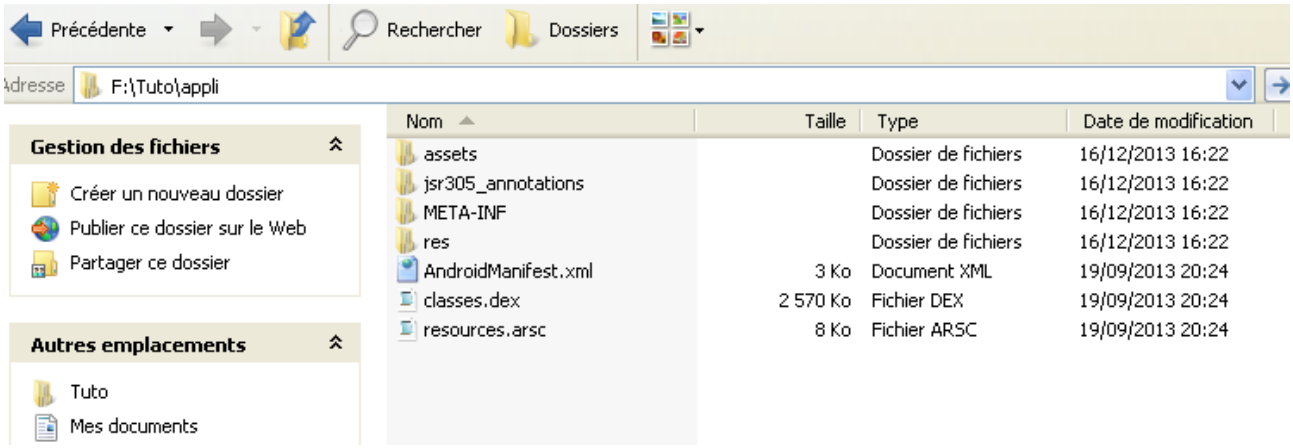
Créez un nouveau dossier et copiez y appli.apk

Info : Nous on ne va pas s'intéresser aux ressources de l'appli beaucoup de tutos en parlent on s'attaque au classes.dex le « coeur » de l'appli.



PHASE 2 : Désassemblage

On renomme le fichier en .rar et on décompresse (winrar / 7zip)



Ok, Copier baksmali.jar et smali.jar dans le dossier juste avant.

On va désassembler le classes.dex avec baksmali.jar

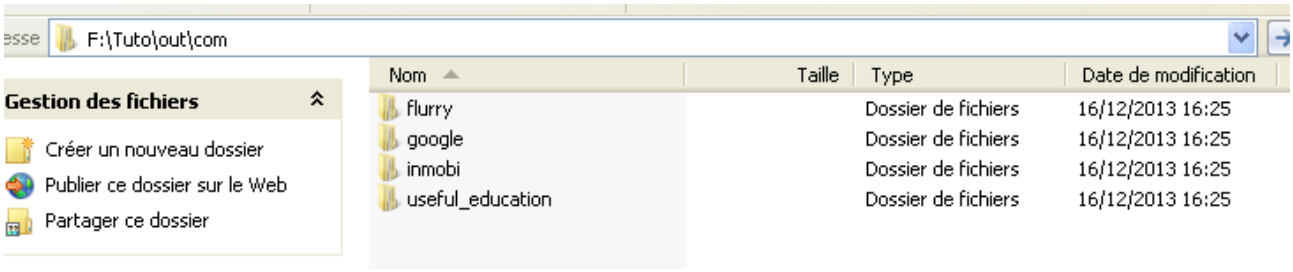
```
F:\Tuto>java -Xmx512m -jar baksmali-2.0.2.jar appli/classes.dex
```

Le prog nous a crée un fichier « out/ » qui contient notre classes.dex désassemblé.

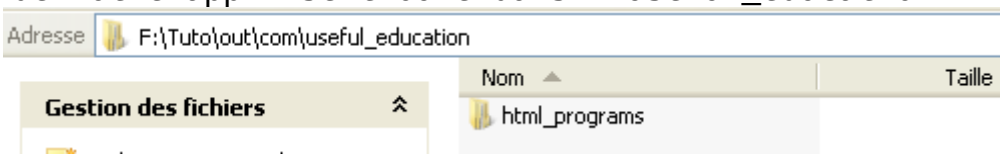
PHASE 3 Le Patch :

Mon but : **Enlever les PUBs de l'appli**

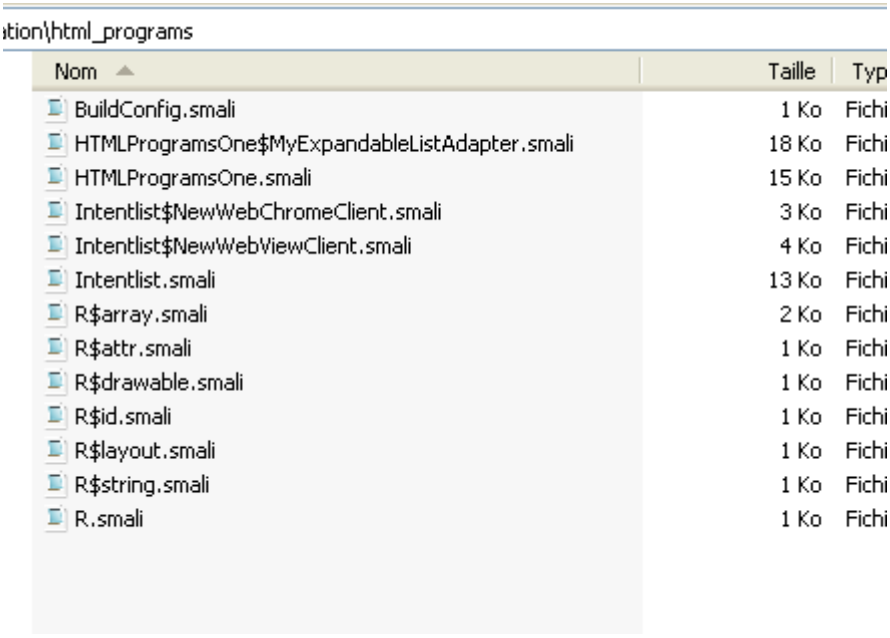
On obtient ceci :



Le cœur de notre appli se trouve dans « useful_education »



On retrouve le nom de notre appli de base « html_programs »
On ouvre :



En fouinant un peu je comprends que « HTMLProgramsOne.smali » est l'élément central du prog.

On ouvre :

```
.class public Lcom/useful_education/html_programs/HTMLProgramsOne;
.super Landroid/app/ExpandableListActivity;
.source "HTMLProgramsOne.java"

# interfaces
.implements Lcom/flurry/android/FlurryAdListener;
.implements Lcom/google/ads/AdListener;


# annotations
.annotation system Ldalvik/annotation/MemberClasses;
    value = {
        Lcom/useful_education/html_programs/HTMLProgramsOne$MyExpandableListAdapter;
    }
.end annotation


# instance fields
.field private interstitial:Lcom/google/ads/InterstitialAd;

.field list:Landroid/widget/ExpandableListView;

.field mAdapter:Landroid/widget/ExpandableListAdapter;

.field mBanner:Landroid/widget/RelativeLayout;

.field metrics:Landroid/util/DisplayMetrics;
```

Il est loin notre assembleur ….

Bon je lis un peu tout ça et trouve ceci :

```
  const-string v1, ""

  const-string v2, "on create"

  invoke-static {v1, v2}, Landroid/util/Log;->e(Ljava/lang/String;Ljava/lang/String;)I

  .line 109
  invoke-virtual {p0}, Lcom/useful_education/html_programs/HTMLProgramsOne;->adMobBannerAds()V
```

Ahah ! Je cherche comment supprimer la pub et là :

adMobBannerAds()

ad => Pub // **Banner** => Bannière …

Je continue :

```
ethod public onDismissScreen(Lcom/google/ads/Ad;)V
   .registers 2
   .param p1, "arg0"    # Lcom/google/ads/Ad;

   .prologue
   .line 268
   return-void
nd method

ethod public onFailedToReceiveAd(Lcom/google/ads/Ad;Lcom/google/ads/AdRequest$ErrorCode;)V
   .registers 3
   .param p1, "arg0"    # Lcom/google/ads/Ad;
   .param p2, "arg1"    # Lcom/google/ads/AdRequest$ErrorCode;
```

Ho ? Les pubs sont gérées par une API google ?

Google => https://developers.google.com/mobile-ads-sdk/docs/admob/fundamentals

```
# virtual methods
.method adMobBannerAds()V
    .registers 4

    .prologue
    .line 114
    new-instance v1, Lcom/google/ads/InterstitialAd;

    const-string v2, "XXXXxxxXXXXXX"

    invoke-direct {v1, p0, v2}, Lcom/google/ads/InterstitialAd;-><init>(Landroid/app/Activity;Ljava/lang/String;)V

    iput-object v1, p0, Lcom/useful_education/html_programs/HTMLProgramsOne;->interstitial:Lcom/google/ads/InterstitialAd;

    .line 117
    new-instance v0, Lcom/google/ads/AdRequest;

    invoke-direct {v0}, Lcom/google/ads/AdRequest;-><init>()V

    .line 120
    .local v0, "adRequest":Lcom/google/ads/AdRequest;
    iget-object v1, p0, Lcom/useful_education/html_programs/HTMLProgramsOne;->interstitial:Lcom/google/ads/InterstitialAd;

    invoke-virtual {v1, v0}, Lcom/google/ads/InterstitialAd;->loadAd(Lcom/google/ads/AdRequest;)V

    .line 123
    iget-object v1, p0, Lcom/useful_education/html_programs/HTMLProgramsOne;->interstitial:Lcom/google/ads/InterstitialAd;
```

Je trouve la fonction qui déclenche les pubs … et heu technique cradace je del …

```
# virtual methods
.method adMobBannerAds()V
    .registers 4


    return-void
.end method
```

(Il faut aussi virer .prologue sinon ça plante)

Ok, Guys le patch semble bel et bien sale mais finit !

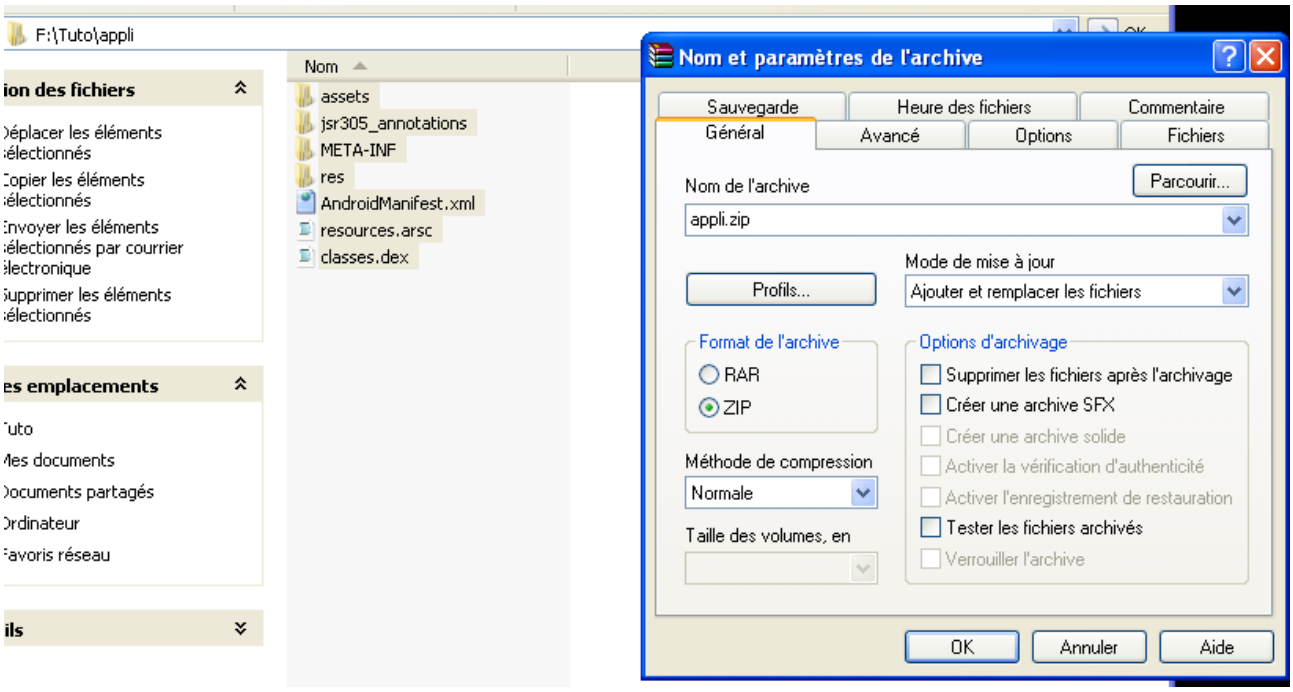
PHASE 4 : RE-ASSEMBLER

```
F:\Tuto>java -Xmx512m -jar smali-2.0.2.jar out/
```

C'est smali qui s'occupe de tout.

Renommer out.dex en classes.dex et remplacer l'original dans « appli/ »

Créer un .zip de tout ça.



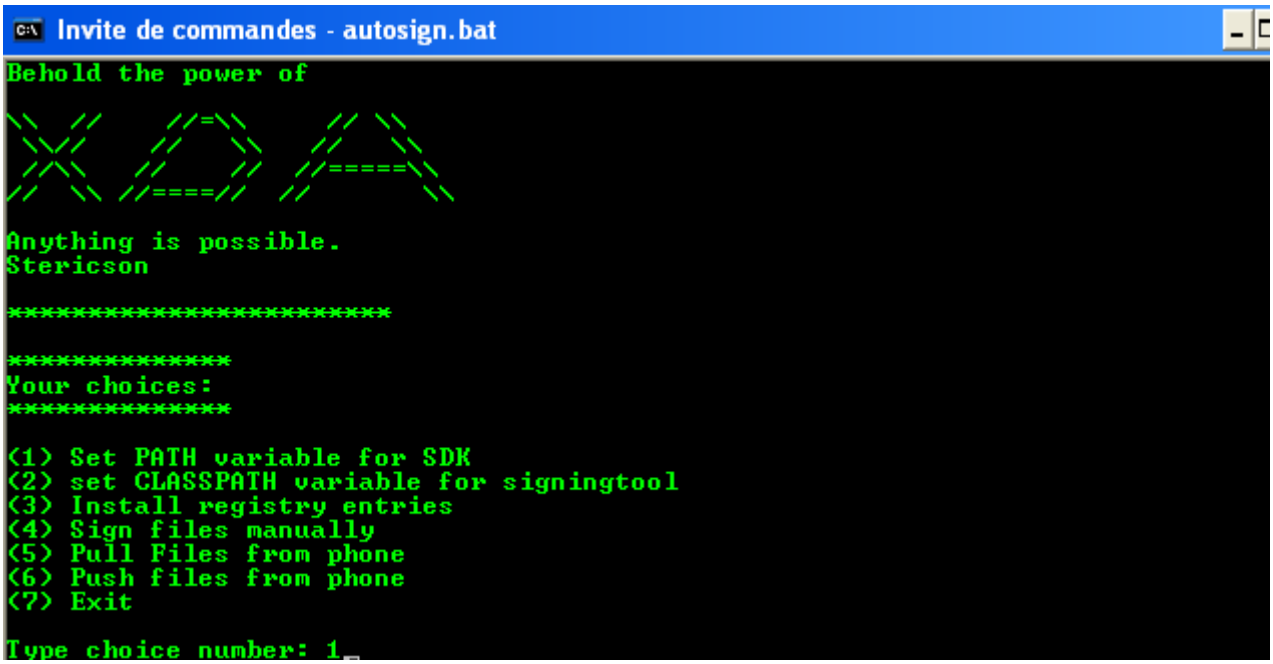
Et renommer l'archive en « appli_patch.apk »

Ce n'est pas finit ! Il faut signer l'.apk sinon … ça ne marchera pas.

PHASE 5 : INSTALLATION Autosign

Décompresser autosign.zip dans le même dossier que « SDK Android »

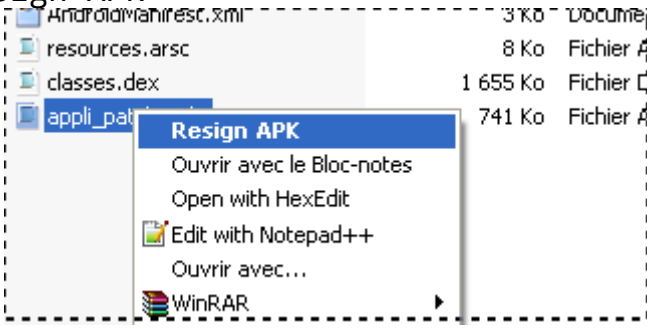
Lancer autosign.bat dans un interpréteur de ligne de commande



Lancer 1, puis 2, puis 3 // et yes à chaque fois.

PHASE 6 : SIGNATURE DU APPLI_PATCH.APK

click droit → Resign APK



PHASE 7 : TEST

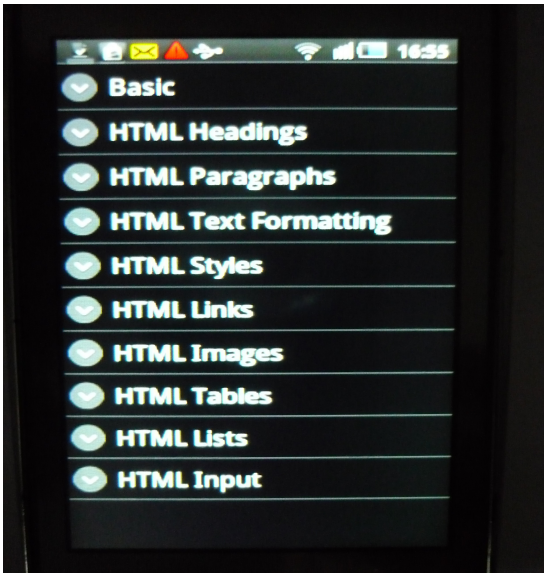
DESINSTALLER VOTRE APP D'ORIGINE AVANT D'INSTALLER CELLE PATCHEE !

Uploader votre patch_appli.apk → ES Explorateur → Toucher Install

Avant :
Au lancement / de façon régulière

Après :

Plus aucune pub !



Par Thxer

Bibli :

http://www.phonandroid.com/forum/comment-decompiler-et-recompiler-avec-l-outil-apktool-t55798.html

http://forum.frandroid.com/topic/124650-tuto-decompilation-modification-recompilation-dapk/

http://forum.frandroid.com/topic/20103-tuto-signer-une-apk-ou-une-archive-zip/

http://wiki.smartphonefrance.info/reversing-android.ashx