ApkCpD

PARA COMPILAR APLICACIONES APK

Autor: Luishiño Pericena Ch

 ApkCpD

Una herramienta para la ingeniería inversa de aplicaciones de Android binarias, de terceros, cerradas. Puede decodificar recursos de forma casi original y reconstruirlos después de hacer algunas modificaciones. También facilita el trabajo con una aplicación debido al proyecto, como la estructura de archivos y la automatización de algunas tareas repetitivas, como la creación de apk, etc.

NO está destinado a la piratería y otros usos no legales. Se podría usar para localizar, agregar algunas funciones o soporte para plataformas personalizadas, analizar aplicaciones y mucho más.

Características

Desmontaje de los recursos a la forma casi originales (incluyendo resources.arsc, classes.dex, 9.png.y XMLs)

Reconstruyendo recursos decodificados de nuevo a APK / JAR binarios

Organización y manejo de archivos APK que dependen de los recursos del framework.

Smali Debugging (Eliminado 2.1.0en favor de IdeaSmali)

Ayudando con tareas repetitivas.

Requerimientos

Conocimientos básicos de Android SDK, AAPT y smali.

Tanto para desarrolladores como para curiosos que quiere conocer que es lo que verdaderamente está pasando dentro del dispositivo y con quién se comunica en el exterior. Podemos tener el código fuente de una aplicación con tan solo unos sencillos pasos. Puede que el código no sea todo lo limpio que nos gustaría pero algo se puede ver.

Resumiendo. Vamos a poder extraer el código siempre y cuando seamos propietarios o tengamos licencia de uso, la información no haya sido expuesta previamente y que la información obtenida no se utilice para la comercialización de un programa sustancialmente similar el cual infrinja los derechos de autor.

Sacar el código de un APK

Si la aplicación es Open Source solo tienes que buscar el código fuente que normalmente se cuelga en repositorios tipo GitHub. Si no es Open Source vamos a tener que hacer lo siguiente:

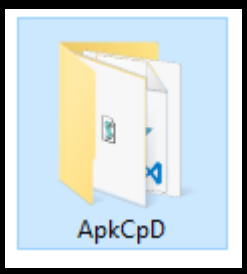
En nuestro caso principalmente es útil para aprender a desarrollar código viendo ejemplos reales.

A partir de aquí hay varios métodos, varios caminos que llevan más o menos al mismo resultado. Aquí os expongo el que me resulta más sencillo.

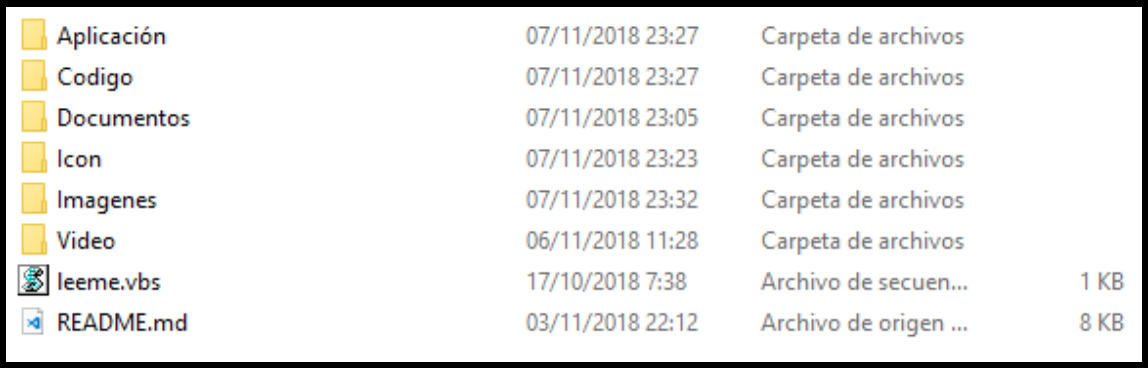
Autor: Luishiño Pericena Ch

Es un programa desarrollado en el lenguaje Bat, que tiene una dependencia de otros programas 7za.exe, apktool.jar, apktool_2.3.3.jar.

- Los programas nos ayudara a poder descomprimir o descompilar las aplicaciones que son desarrollada en Android, con la extensión".apk "para poder modificar el código y mejorar la aplicación.
- Podemos mejorar una aplicación ya que tendremos el código fuente, podríamos infectar una aplicación con virus entre otras cosas. Para eso debes tener conocimiento en programación con el lenguaje Android.

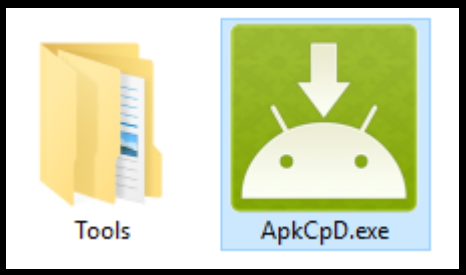


1



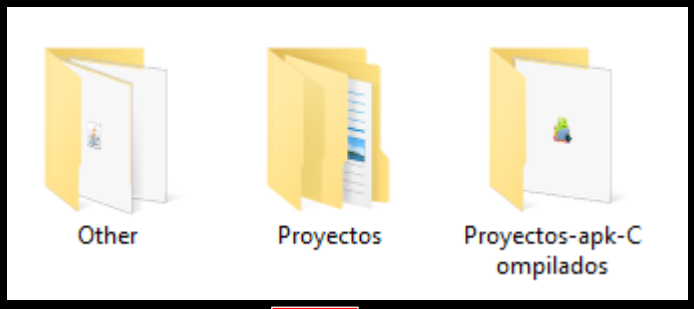
2

Los paquetes de aplicación de Android (APK) es el formato usado para distribuir e instalar aplicaciones en el Sistema operativo para móviles Android de Google. Hay muchas razones por las cuales querrías descompilar un APK, por ejemplo para aprender cómo funciona una aplicación, para incrementar la seguridad y complejidad de tu código, para robar el código fuente de aplicaciones de tercero ... es decir, para analizarlo ... y otras.

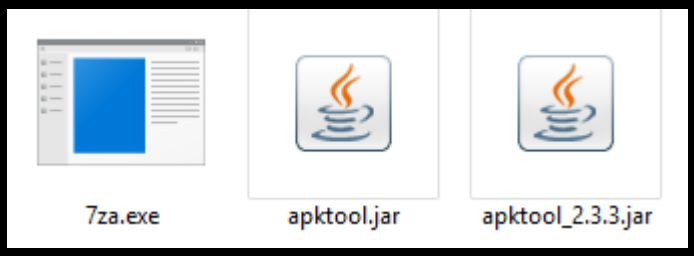


3

Para descompilar un APK, en este artículo usaremos ApkªDcx, la herramienta de líneas de comando e interfaz gráfica (GUI) para obtener el código fuente de archivos DEX y APK



4

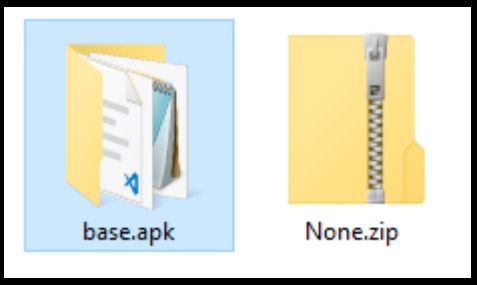


5

Autor: Luishiño Pericena Ch

Las apps Android están escritas en lenguaje de programación java. Diseñado en los años 90 con una filosofía libre similar a Linux (PCs), fue credo para que se pudiera ejecutar en diferentes máquinas virtuales. Es por esto que la mayoría de apps java comprenden una serie de archivos para una mayor compatibilidad con la mayoría de máquinas virtuales.

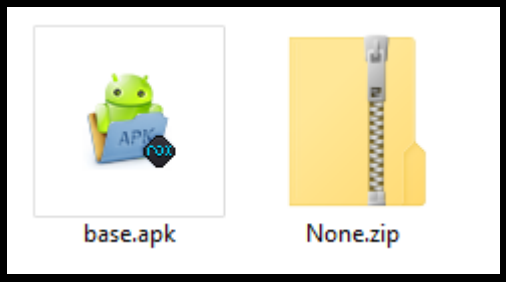
6



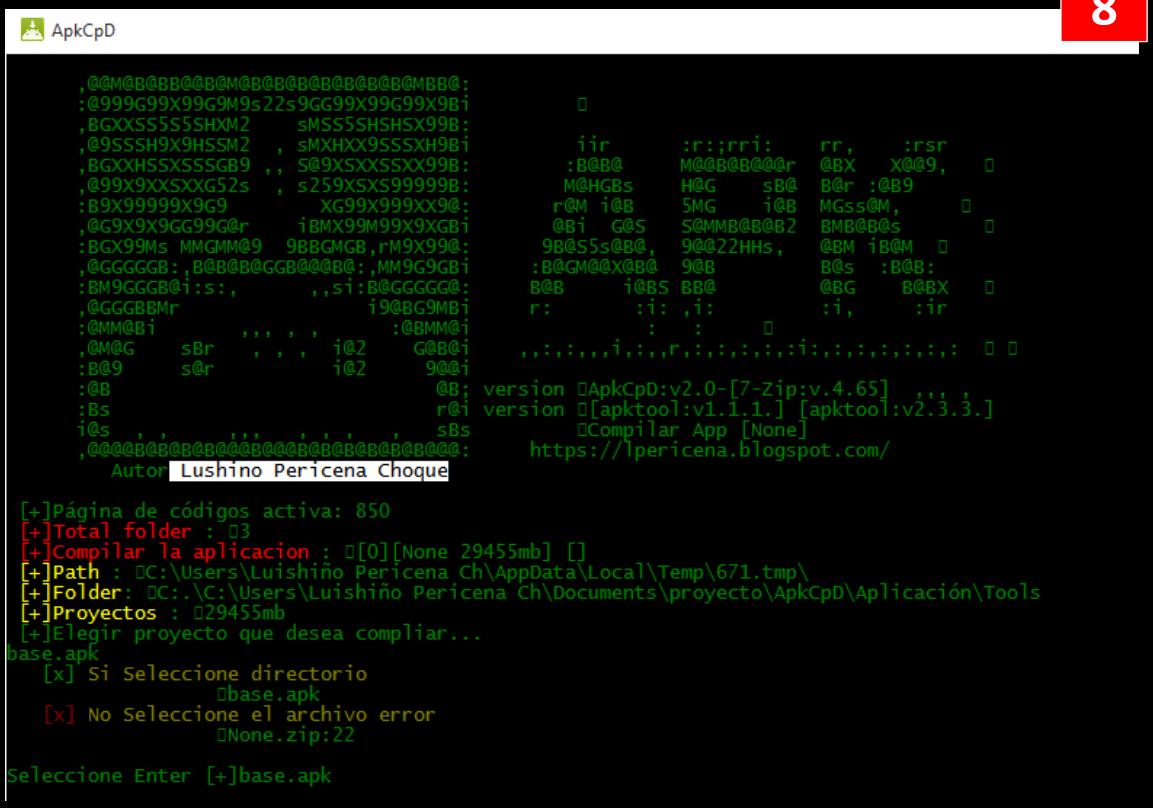
La solución para presentar todos estos archivos en uno solo (aplicacion), no fue otra que compilarlos en un archivo comprimido basado en la compresión Zip o 7zip, ideada años antes que java.

Dicho esto, podríamos decir que las apps Android son archivos comprimidos basados en zip, y hoy en día, la mayoría de compresores/ descompresores estilo WinZip o WinRAR leen la compresión apk como si fuera un formato Zip.

7

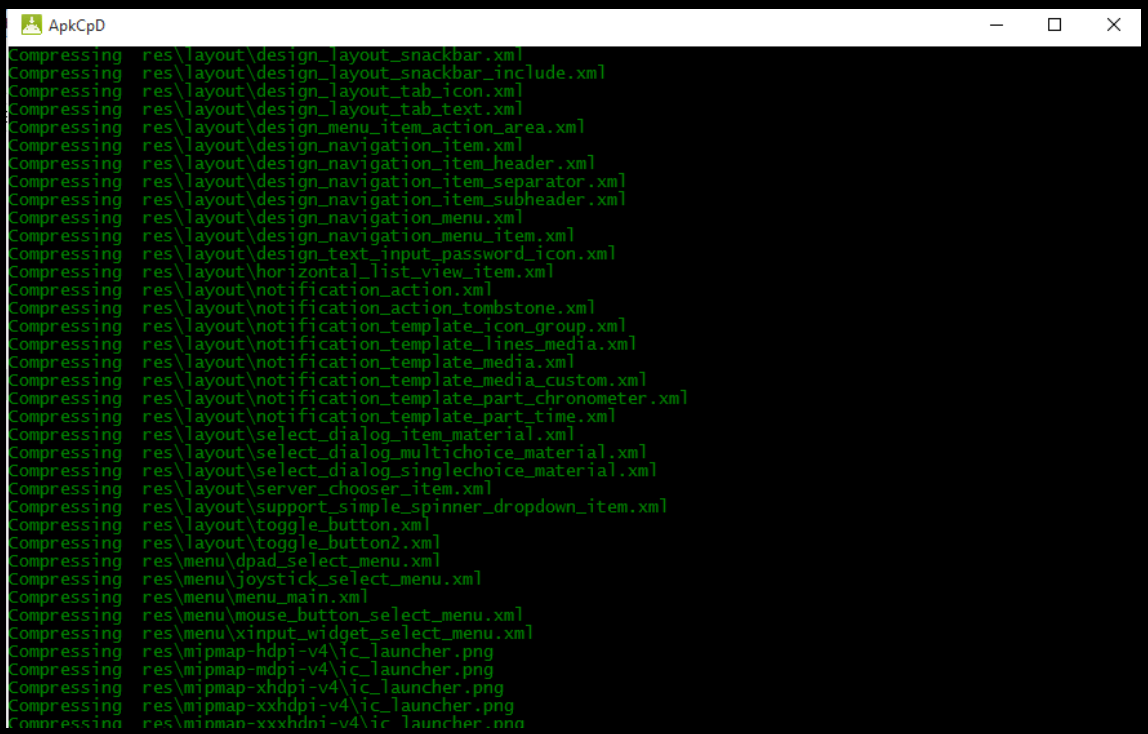


8

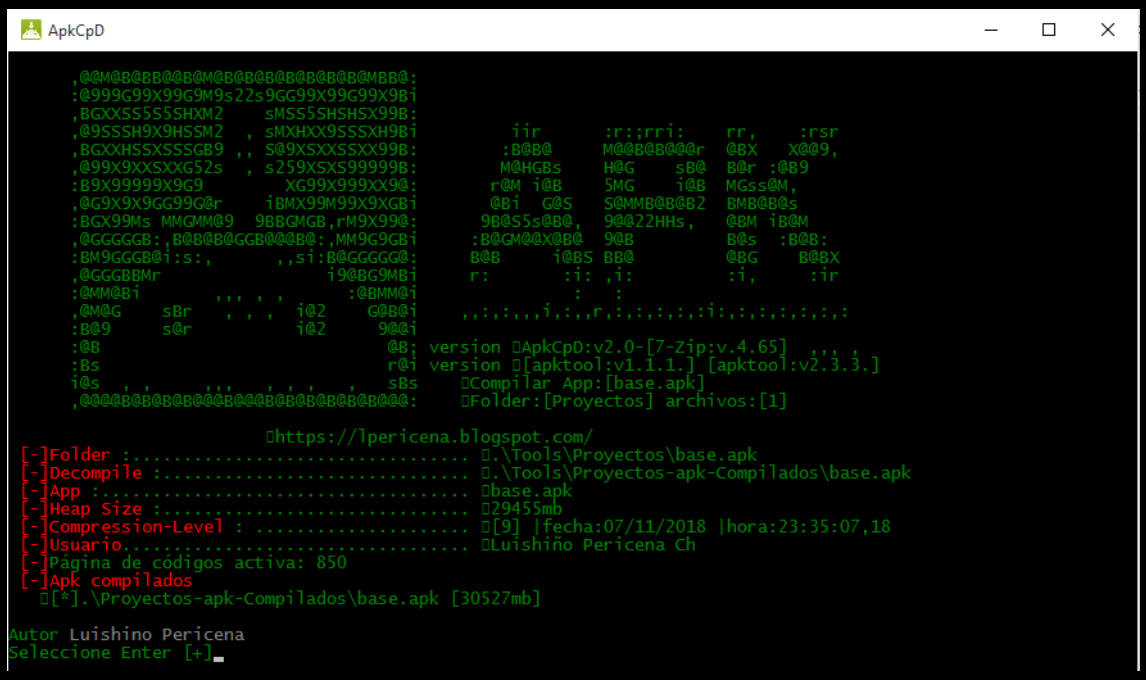


Autor: Luishiño Pericena Ch

9



Autor: Luishiño Pericena Ch



Ingeniería inversa con un archivo APK ¿es legal?

El proceso para conseguir el código de programación desde un archivo ejecutable o cualquier otro archivo ya compilado se denomina ingeniería inversa. La ingeniería normal, por llamarla de alguna manera sería el propio desarrollo del código fuente.

Para poder leer el código de un archivo con extensión .apk necesitamos varias herramientas y para empezar necesitamos el susodicho archivo APK de la aplicación. Para conseguirlo podemos buscarlo en los repositorios de aplicaciones online o si tenemos la aplicación instalada en el dispositivo podemos extraer la APK desde un explorador de archivos.

Descargar

- ✓ https://github.com/Pericena/ApkCpD
- ✓ **https://lpericena.blogspot.com/2018/11/ApkCpD.html**