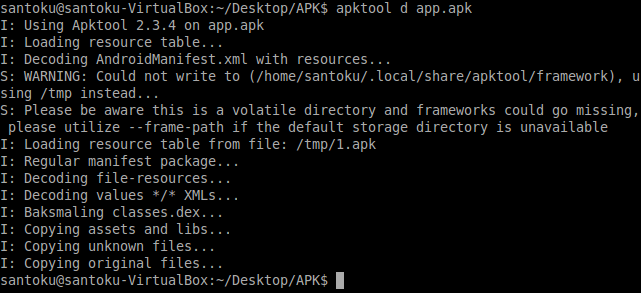
CDM – Practica 3 Modificacion y repaking de APK

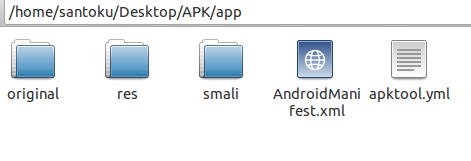
Nombre : Adrian Tendero Lara

El ejercicio propuesto consiste en alterar el código smali del apk dado en la practica 3 consiguiendo que la aplicación pase de la actividad principal a la segunda actividad sin pasar por la actividad de loging (donde se comprueban las credenciales).

Para esto primero tenemos que desempaquetar el apk objetivo, para ello usamos el comando apktool d <APK> como se muestra en la imagen.



Esto nos genera una carpeta que incluye el manifest, los recursos y el código smali



Para realizar las modificaciones pedidas nos tenemos que ir ha app/Smali/es/upv/cdm/jcruizg/holamundo/MainActivity$1.smali que contiene entre otras cosas el código que utiliza el botón login para pasar de la mainActivity ha la loginActivity como se puede comprobar aquí.



Como nos pide el ejercicio que modifiquemos la app para que utilizando ese botón en vez de ir a la LoginActivity pasemos ha ir a la SegundaActividad (que requiere authentificacion) entonces tendremos que modificar el código anterior para que vaya a la segundaActividad.

Por tanto cambiamos el valor de v2 contenido en esta línea.



Por este contenido



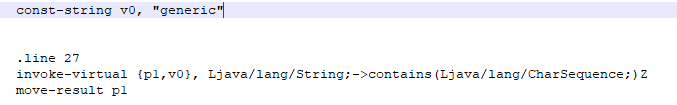
(Nota esta línea la he sacado de la app “completamente resulta del ejercicio”)

También nos pide que implementemos un heurístico de evasión para que la aplicación funcione correctamente en emuladores y funcione en modo haqueado cuando se ejecute en un dispositivo real.

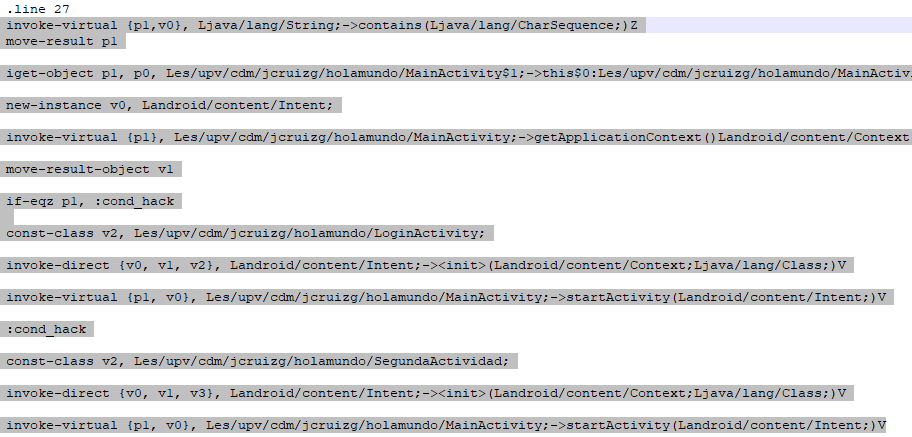
Para esto primero tenemos que obtener el nombre del dispositivo donde se ejecuta la app.



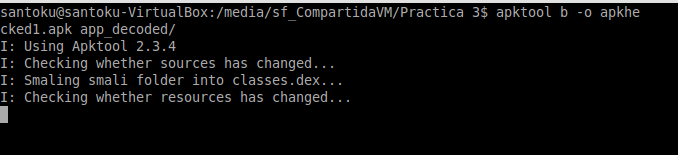
Y después comprobar si el dispositivo Android donde se ejecuta es un tipo “genérico” que implica que es un emulador.



Y simplemente poniendo un if-else de smali podemos ajustar el comportamiento de la app dependiendo de si es un emulador o un dispositivo real.



Ahora nos queda empaquetar y probar la app modificada



Alinearla

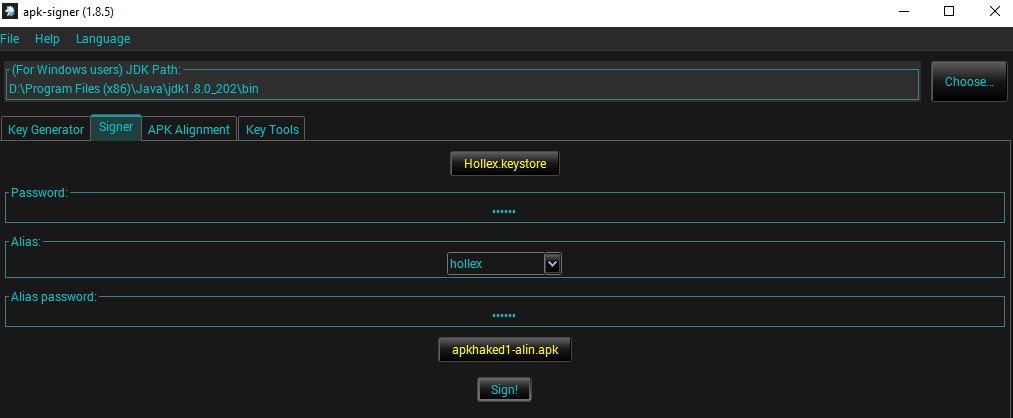


Y firmarla, aquí es donde ha cosa me ha estado dando problemas ya que mi santoku no tiene el apksigner como se puede ver en la siguiente imagen.



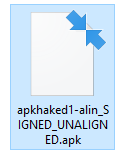
Para ello me he visto obligado ha descargarme otra aplicación para poder firmar manualmente, ya que ni actualizando el santoku (los apktools) ni ningún otro método me ha ayudado.

Esto lo realizo en mi maquina host, no en santoku.



(\* Nota: Hollex es mi alias de internet como podrás comprobar si vas ha mi repositorio de github donde se encuentran todas las practicas de cdm \*)

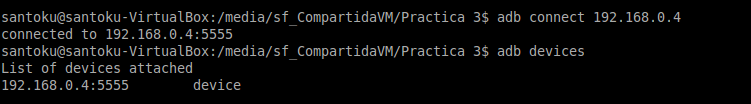
Con esto ya tenemos nuestro APK firmado.



Como ves el programa dice que esta Unaligned, pero ya realice dicho paso antes, así que simplemente le cambio el nombre y punto ya que el proceso de firma no tendría que cambiar nada.

Y ahora solo nos queda instalarla en el emulador y probarlo.

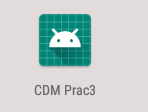
Para ello conectamos el Android con nuestro santoku



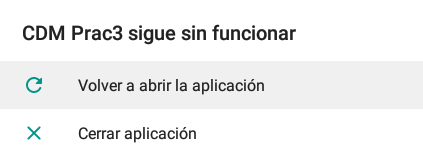
Y instalamos el apk



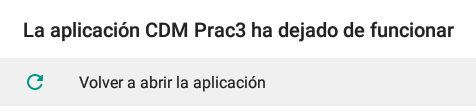
Y ya tenemos la aplicación haqueada instalada en nuestro Android.



Pero tengo problemas y no puedo probarla



Asique vuelvo ha probar ha alinear el apk firmado tal como nos decía al aplicación de firmado y obtenemos el mismo resultado.



En teoría tendría que haber funcionado y implementa todo lo pedido por la practica 3.