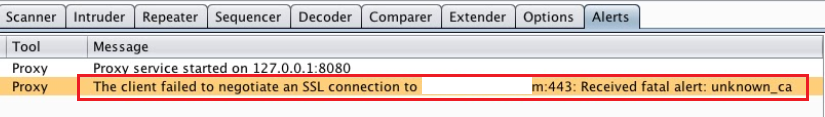
**SSL Pinning** **bypass using code manipulation**

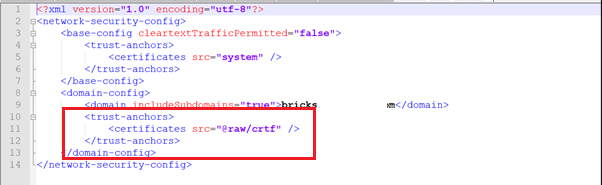
First try to capture app traffic. If SSL Pinning is implemented then you will get certificate error.

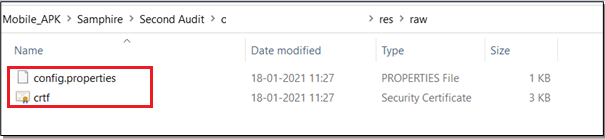


Follow below steps to bypass Root detection by modifying application source code

1. Decompile the Application using APKTool and JADX
2. Find the source code or configuration file related to SSL Pinning

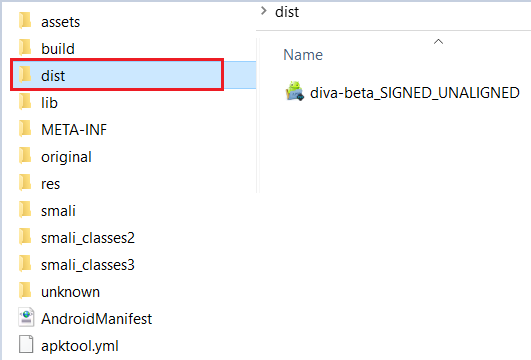




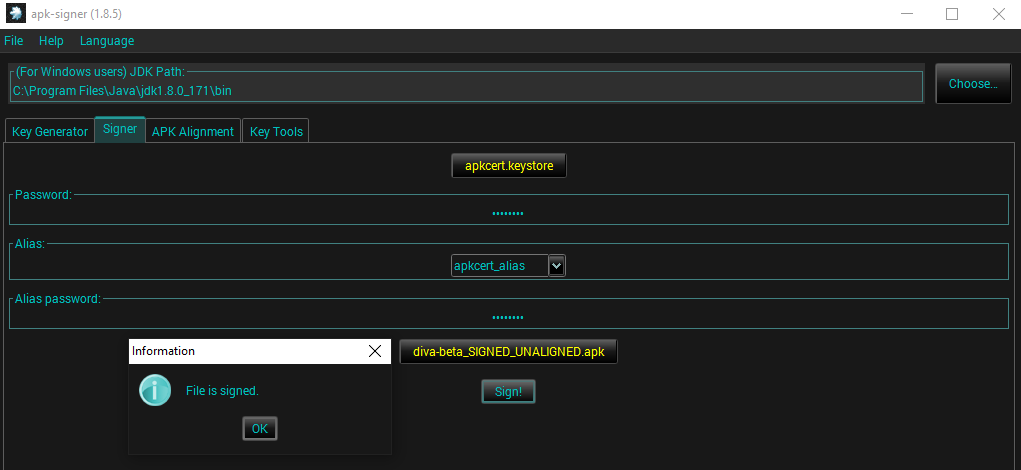


1. Remove the certificate code from configuration file (Android Manifest.xml) or rename and replace your proxy tool certificate in raw directory.
2. Compile the modified Application code using APKTool. It will generate new APK file under dist folder. Use below command to compile app.

apktool b <app\_package>



1. Sign the modify Application APK using APK-Signer utility.





1. Install modified SSL Unpinned APK file and try to capture app traffic

The following screenshot shows that SSL Pinning is bypassed successfully and we are able to capture https traffic in proxy tool

