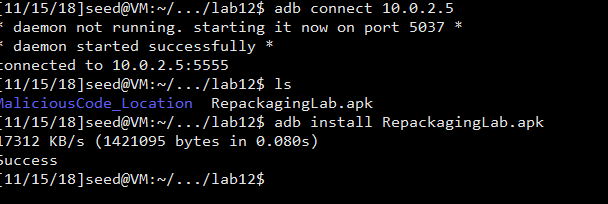
Android Repackaging Attack Lab

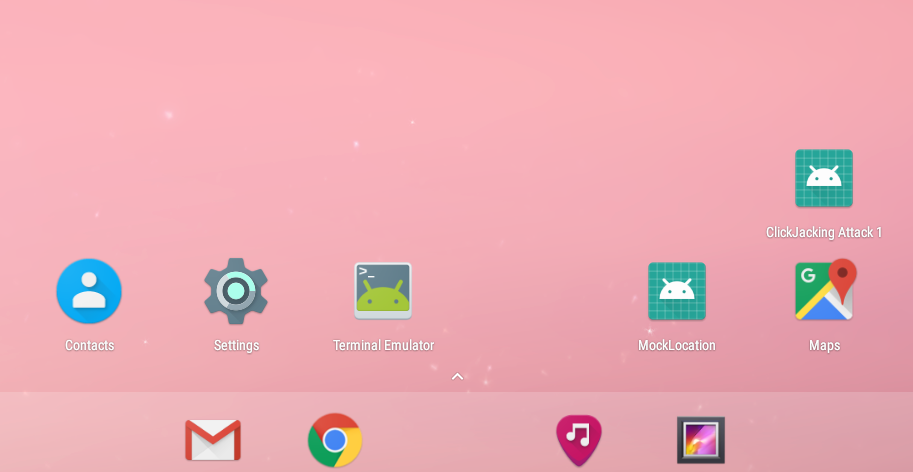
## Task 1: Obtain An Android App (APK file) and Install It

Firstly, find the ip address of the android VM:



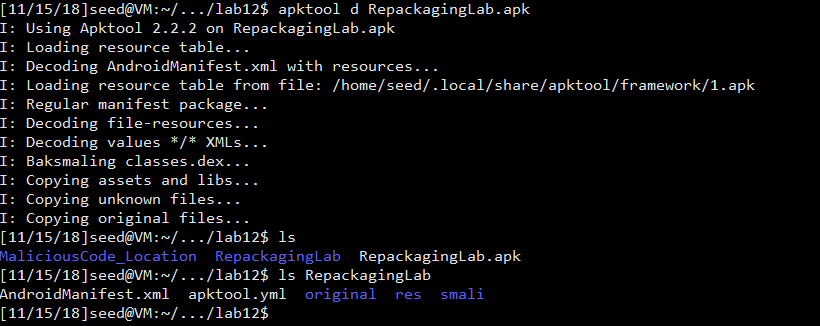
We can see that the ip address is 10.0.2.5. And the ip address of my ubantu is 10.0.2.6





As we can see, the APK file is installed successfully via the adb connection.

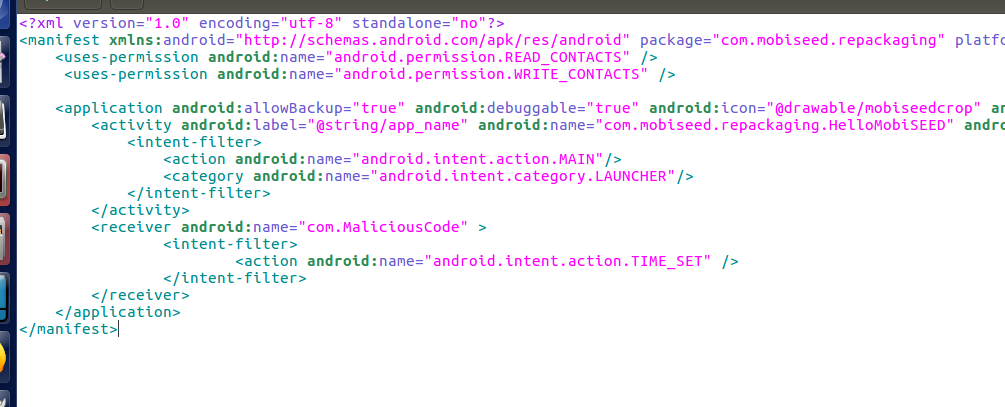
## Task 2: Disassemble Android App



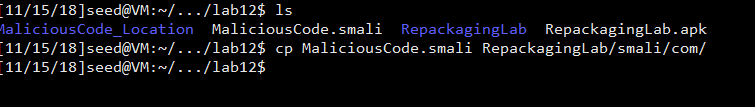
After running the decode instruction of apktool, the apk file is decoded into a folder with several files and child folders.

## Task 3: Inject Malicious Code

Modify the xml file:



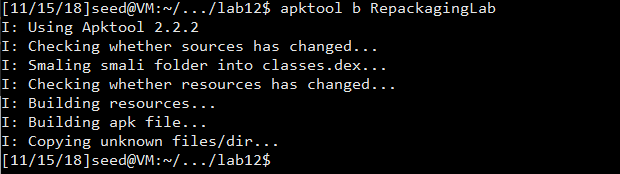
Copy the malicious code to the smali/com folder



## Task 4: Repack Android App with Malicious Code

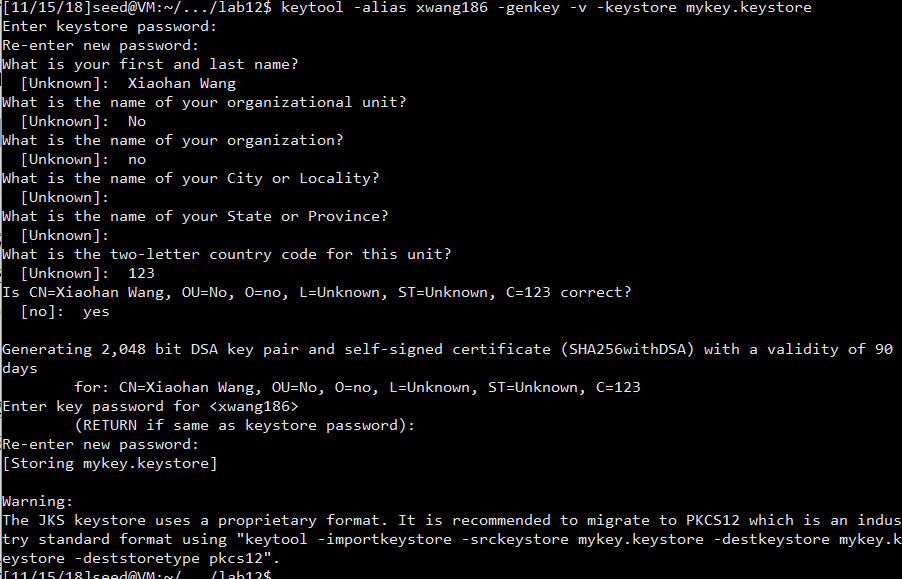
### Step 1: Rebuild APK

apktool b RepackagingLab



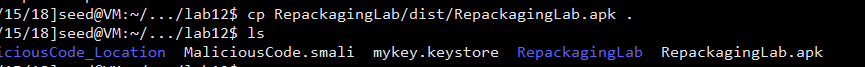
### Step 2: Sign the APK file

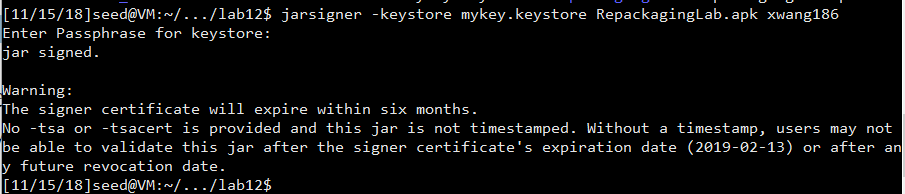
keytool -alias xwang186 -genkey -v -keystore mykey.keystore



Create the key pair

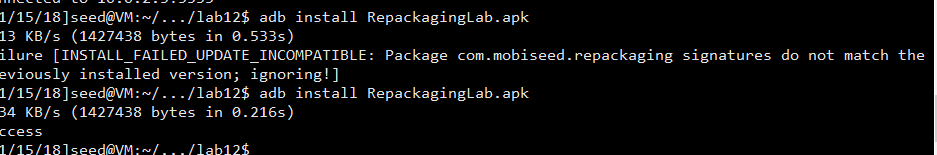
jarsigner -keystore mykey.keystore RepackagingLab.apk xwang186





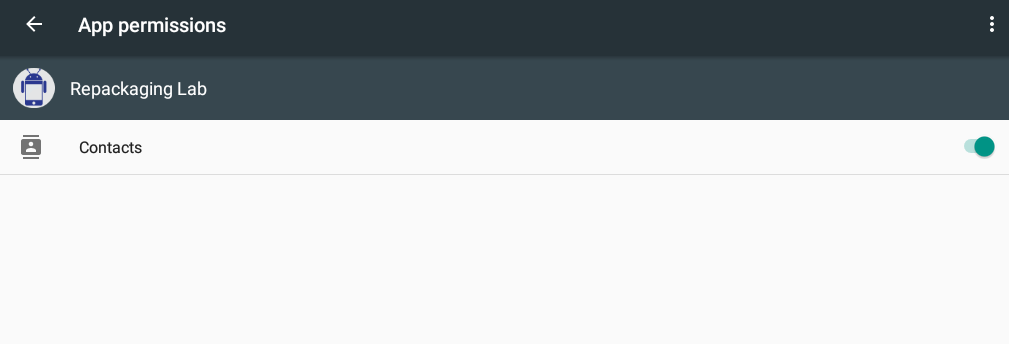
Sign the apk successfully

## Task 5: Install the Repackaged App and Trigger the Malicious Code

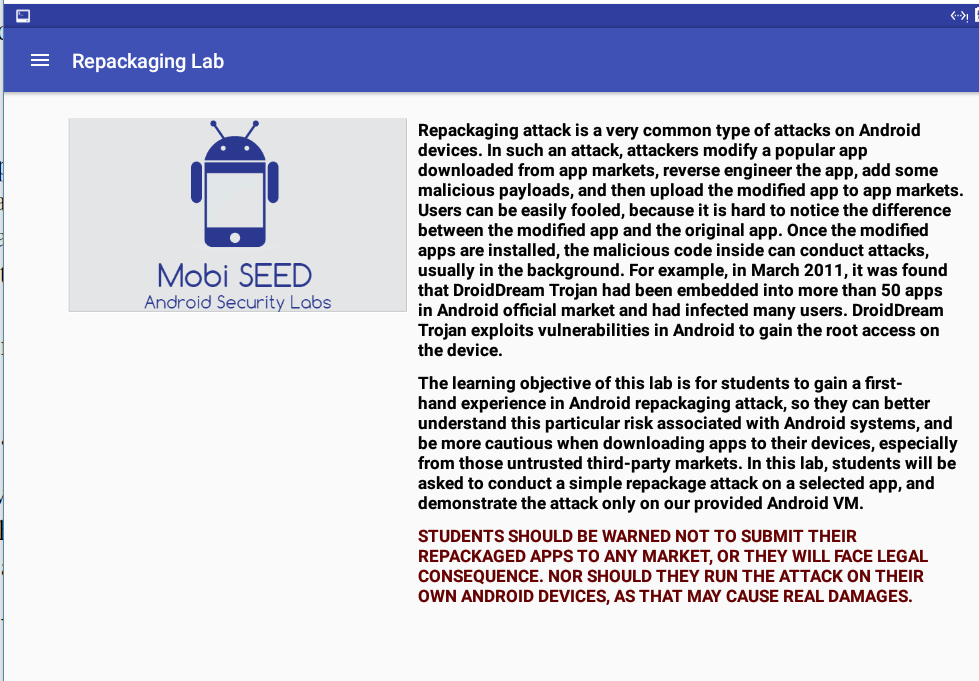


Install the new apk file. If we don’t uninstall the old version, the modified version will not be recognized.

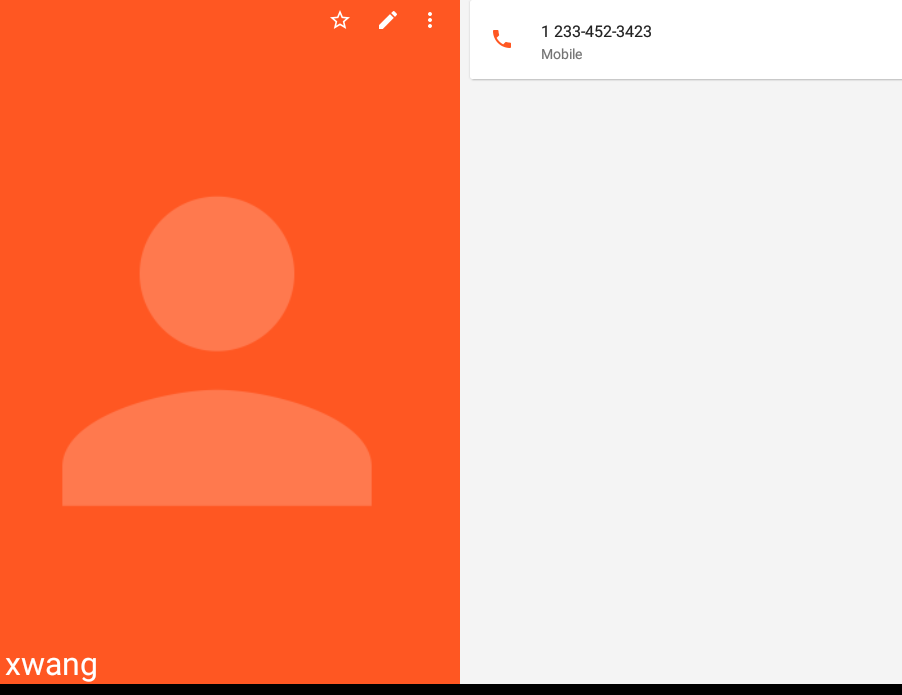
Change the permission of the apk:

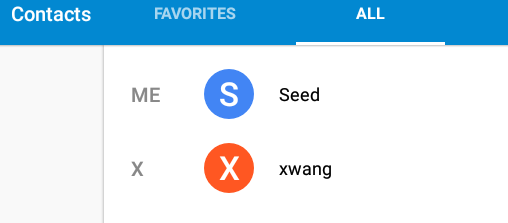


Firstly, run the application once.

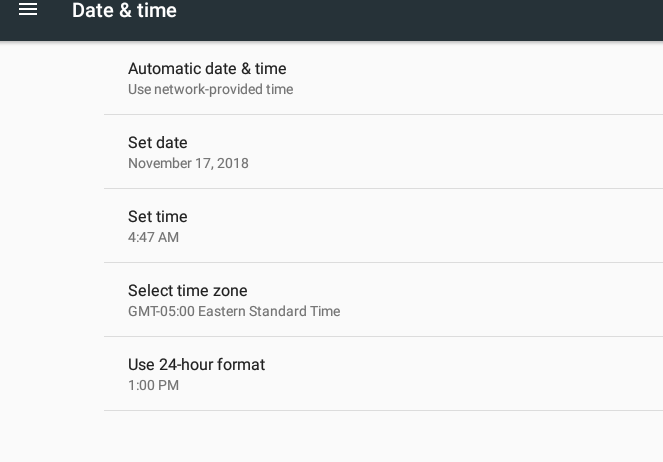


Add contacts:

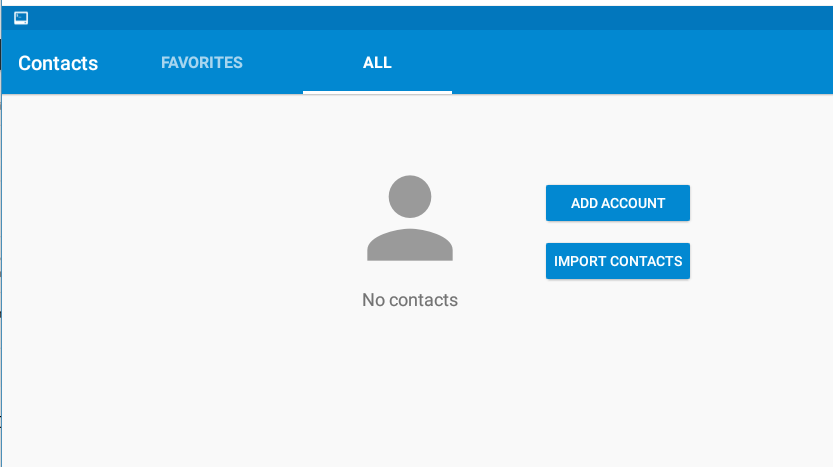




Change system time:



Changed the date and time.

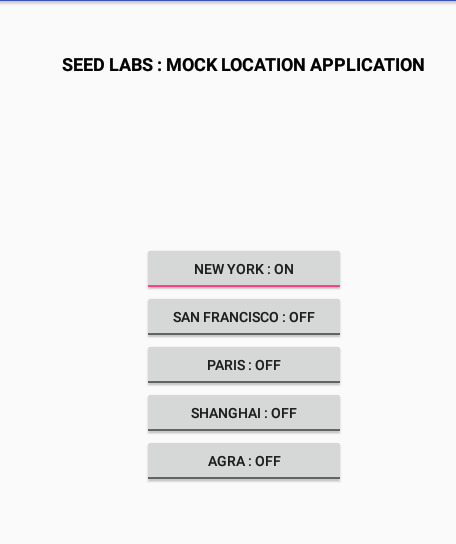


Go back to the contact list and find that there are no contacts anymore, which means the task succeeds.

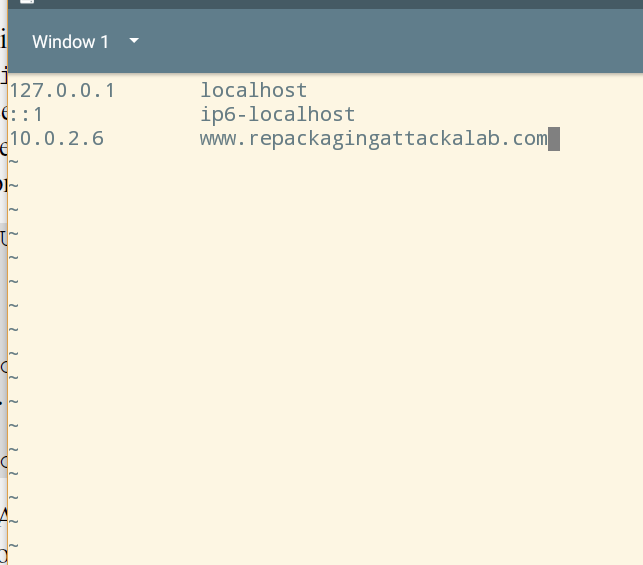
In the malicious code, the onReceive function implements the operations of delete contacts. To invoke that, we change the xml file to add the receiver. As well, we give the application the permission to read and write contacts. As a result, the application can delete all the contacts.

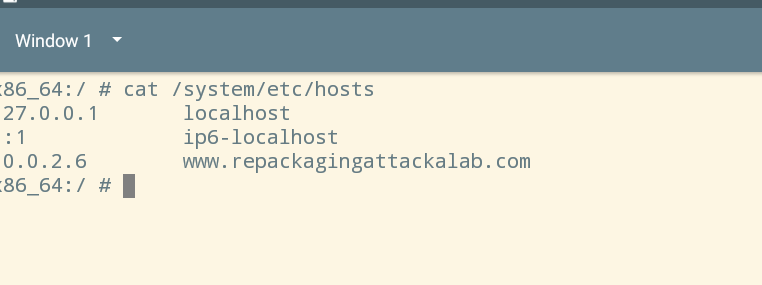
## Task 6: Using Repackaging Attack to Track Victim’s Location

### Step 1. Setting up mock locations.



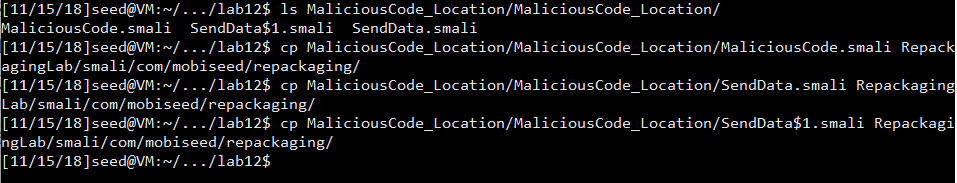
### Step 2: Configuring DNS.



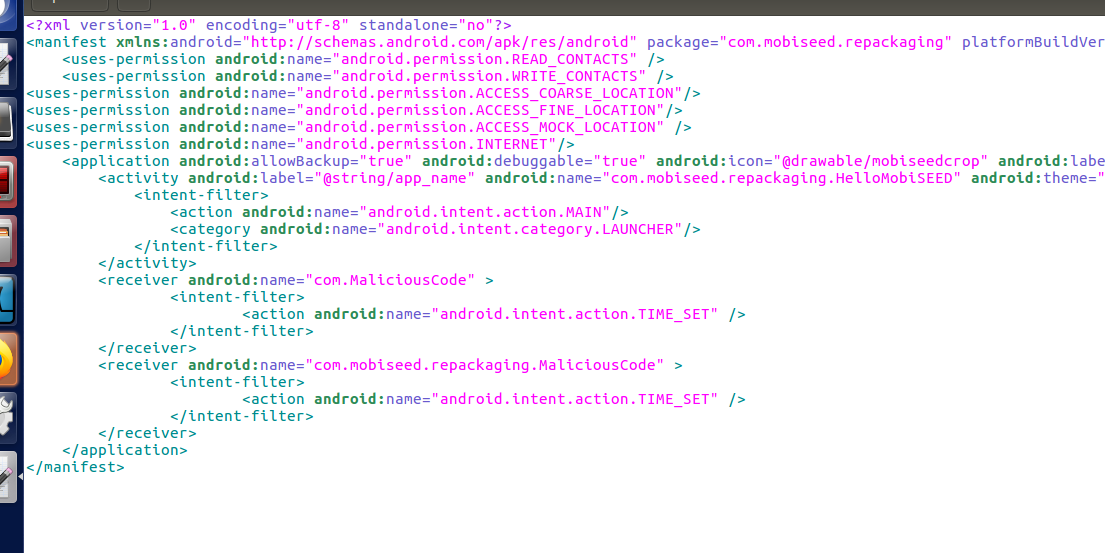


### Step 3: Repackaging and installing the victim app.

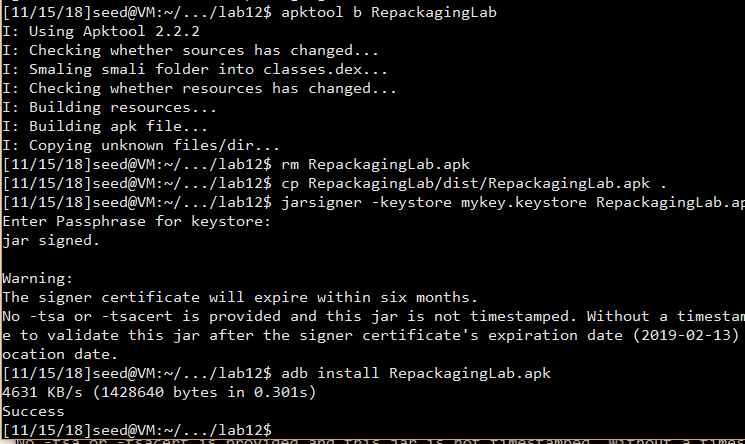
Firstly, place the three malicious files in the folder smali/com/mobiseed/repackaging/



Modify the xml file:

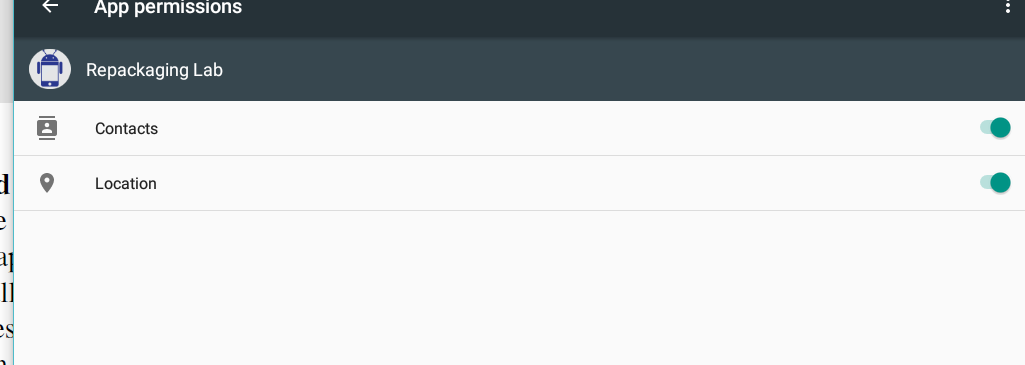


Then, repack, re-sign and install.



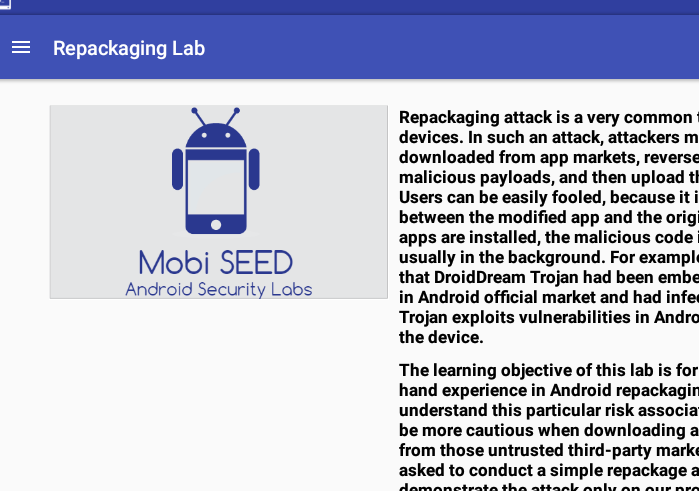
### Step 4: Enabling the permission on the Android VM.

Enable the permission of getting Location



### Step 5: Triggering the attacking code.

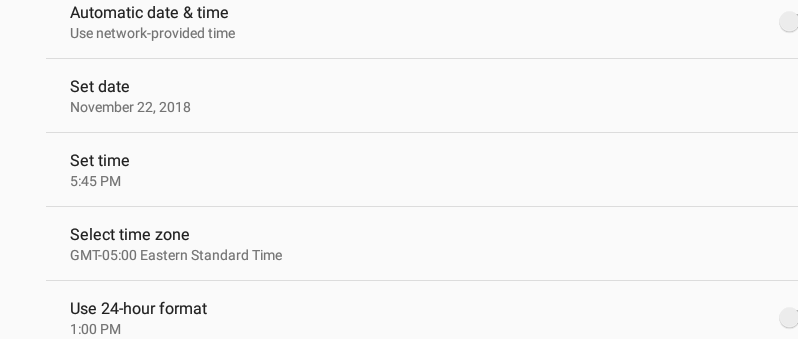
Open the application



Change the location in mock location application:

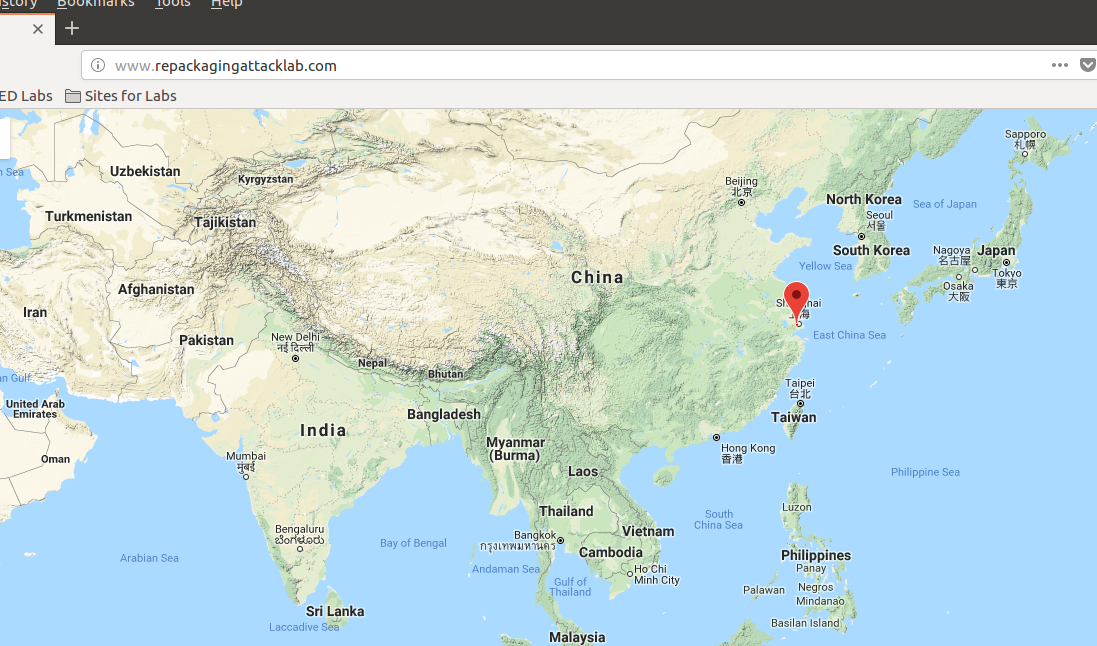


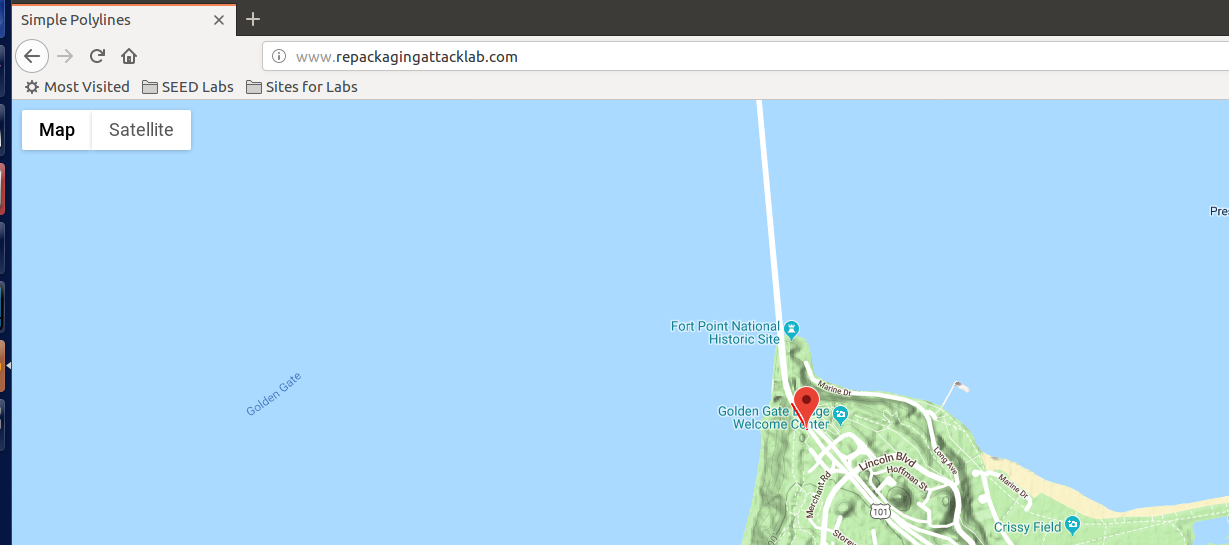
Change the System time:



Repeat multiple times.

Then, go to the ubuntu VM to check the result:





As we can see, the location changes whenever we mock a new location and set the time. The receiver has a SET\_TIME listener, whenever we set the time, the malicious code invokes. In the malicious code, we send the new position to the server [www.repackagingattacklab.com](http://www.repackagingattacklab.com). Since we have set the DNS, the address becomes the ubuntu’s address. In the ubuntu server, when it receives new locations, it goes to the google map with the new location as default.