**Android Repackaging Lab**

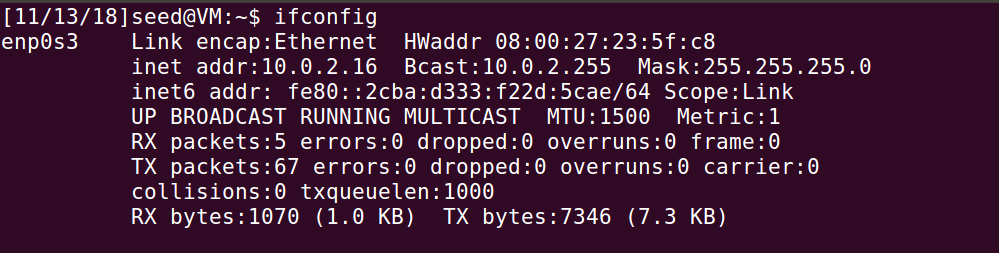
**Karan Amrutesh**

**Lab Environment Setup:**

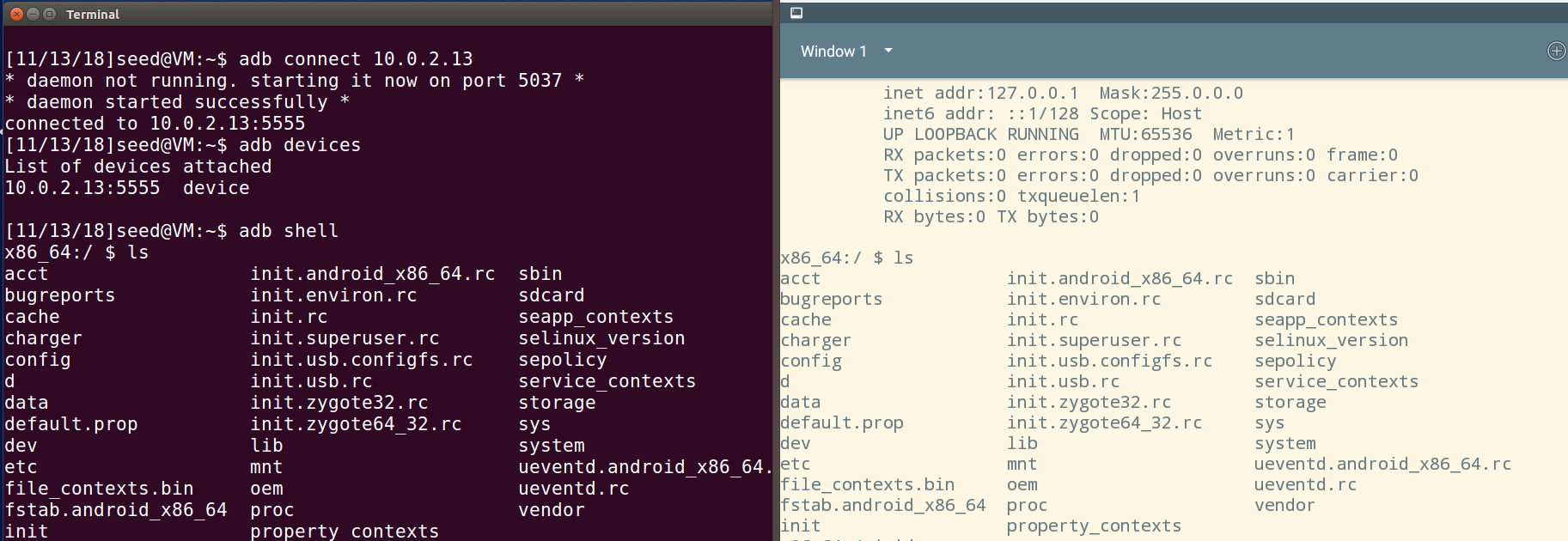
* After doing the NatNetwork setup, we get the IP address of our android VM.
* Using the terminal emulator app, we get the IP address of our android VM to be 10.0.2.13:



* IP address of our SEEDUbuntu VM is 10.0.2.16:

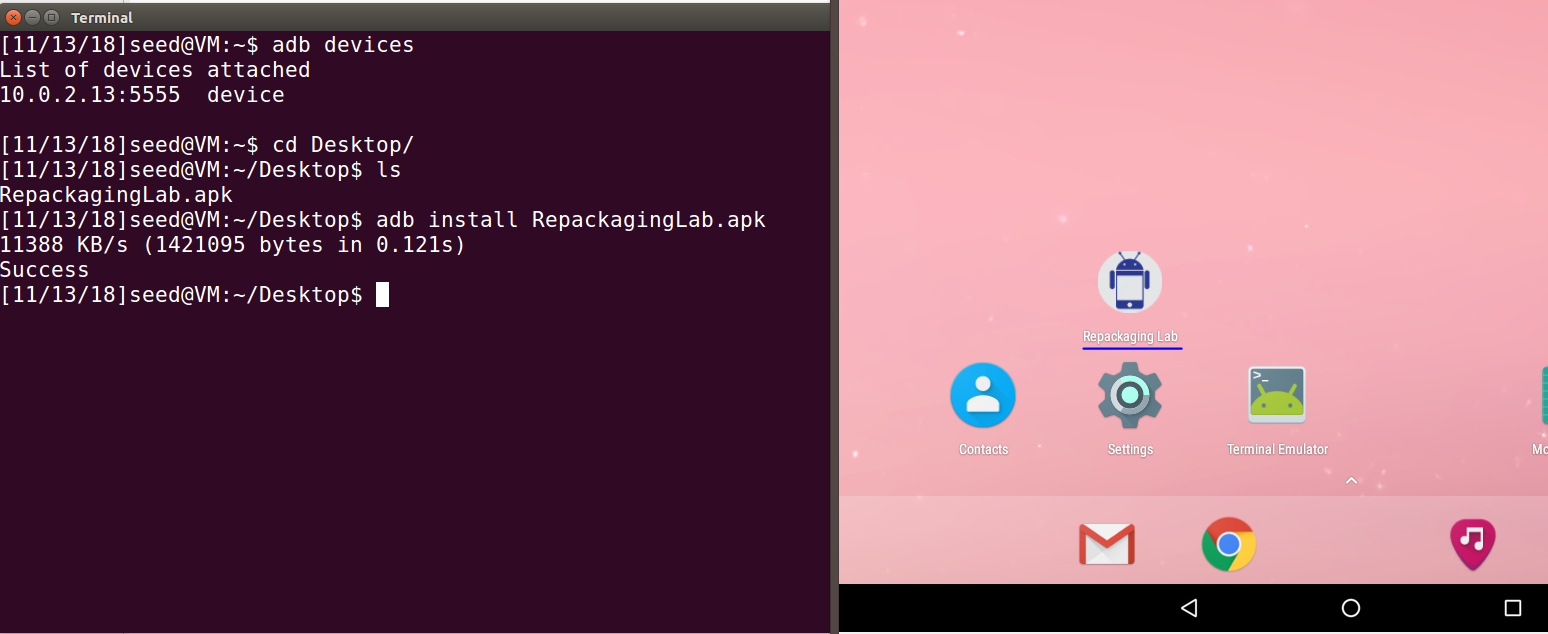


* We use the adb connect command to connect to the android VM.
* We use the adb shell command to get the shell prompt of the android VM:



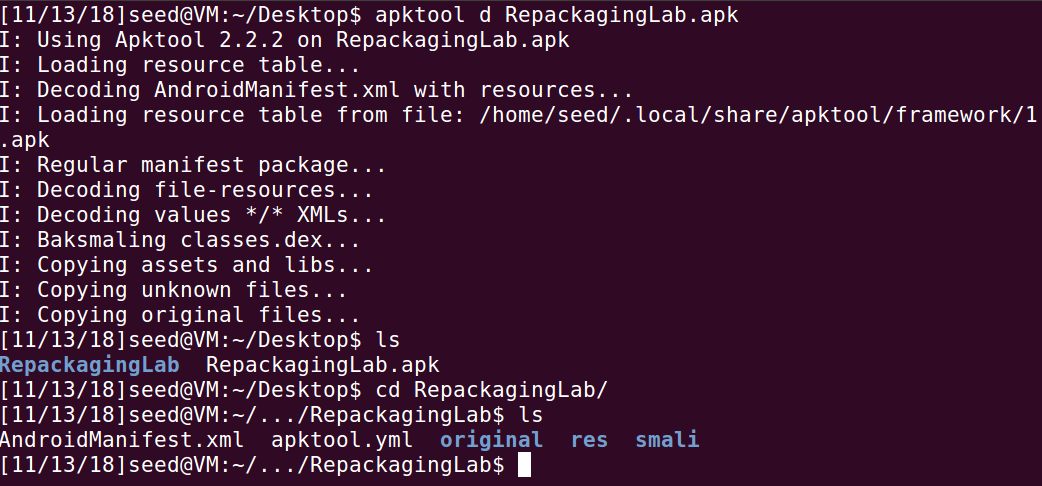
**Task 1: Obtain An Android App (APK file) and Install It:**

* Installing the RepackagingLAb.apk onto the android VM using the adb command:



**Task 2: Disassemble Android App**

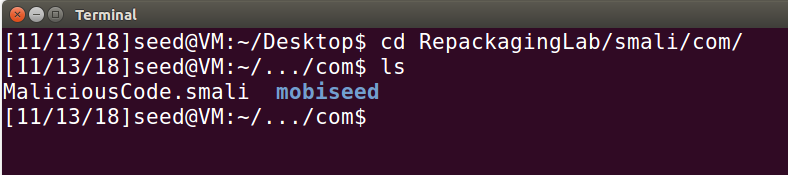
* We disassemble the RepackagingLab.apk using the apktool:



* We can see that the apk has been disassembled into the folder RepackagingLab

**Task 3: Inject Malicious Code**

* Placing our malicious code inside the /smali/com/ folder:

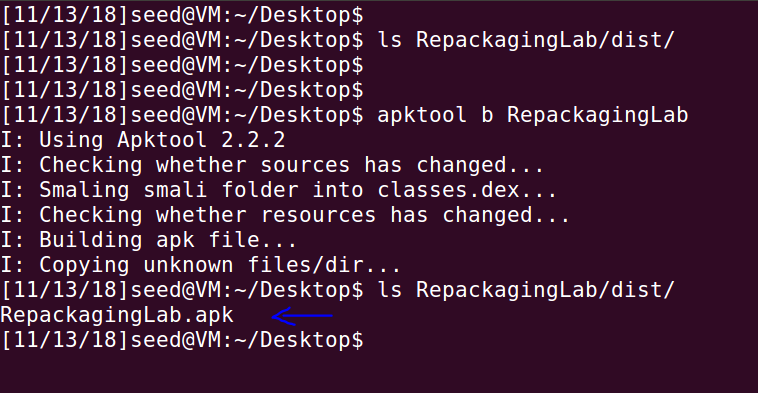


* Modifying the AndroidManifest.xml file to register our broadcast receiver to the system and giving the app, permissions to read and write the contacts:

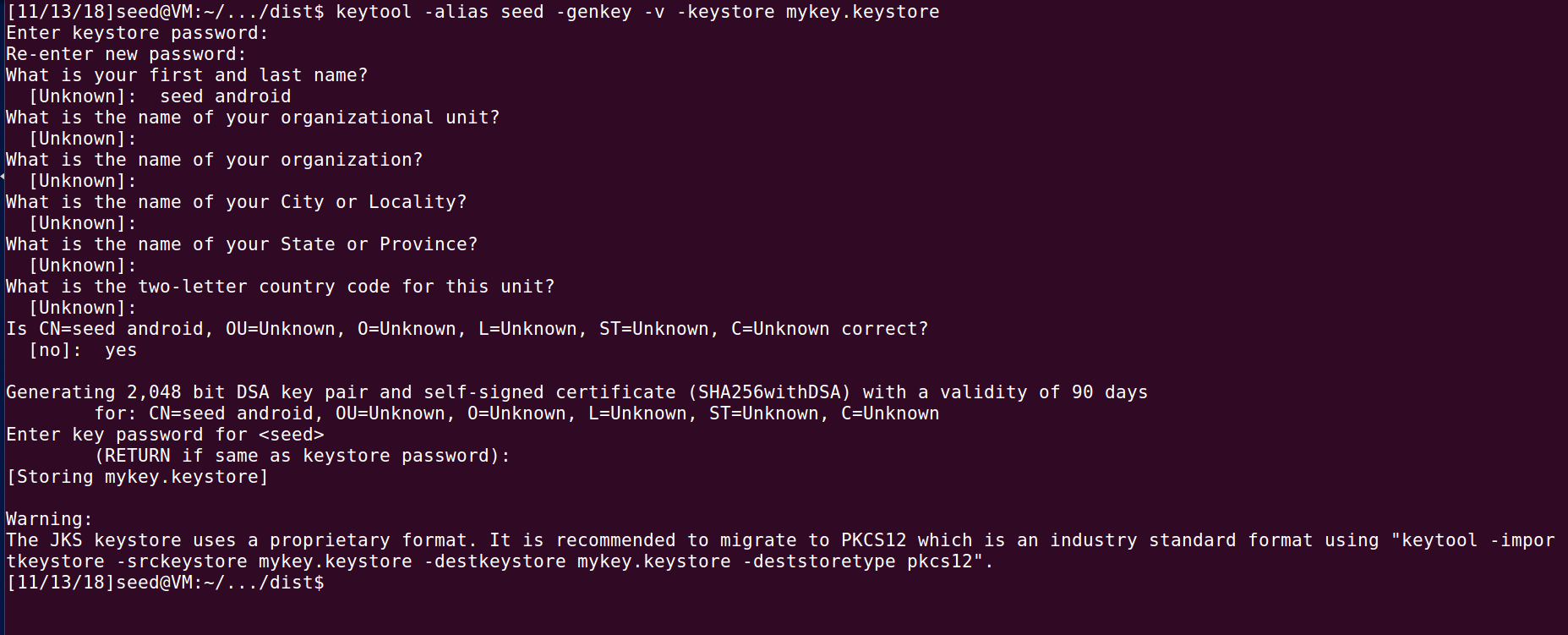


**Task 4: Repack Android App with Malicious Code:**

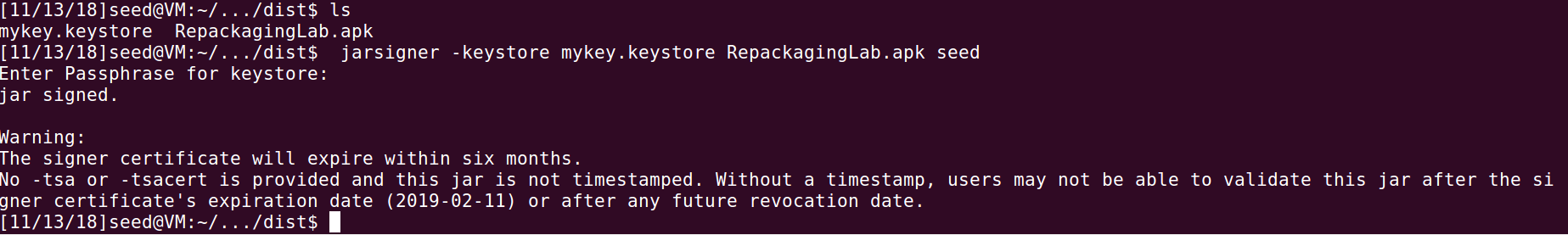
* We repack the android app with our malicious code using the apktool:



* Then we sign the APK file: First we generate a public and private key pair using the keytool command:

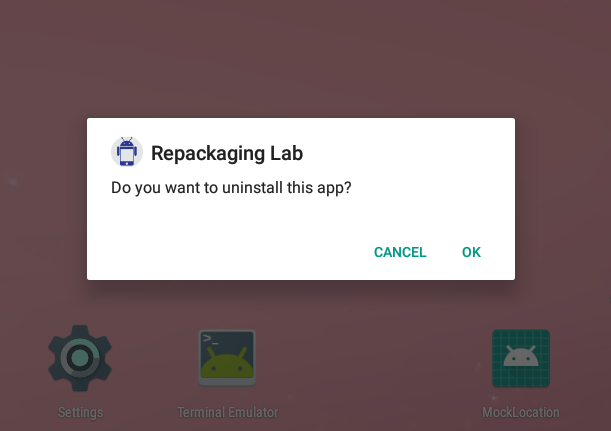


* Then we use *jarsigner* to sign the apk file using the key generated in the previous step

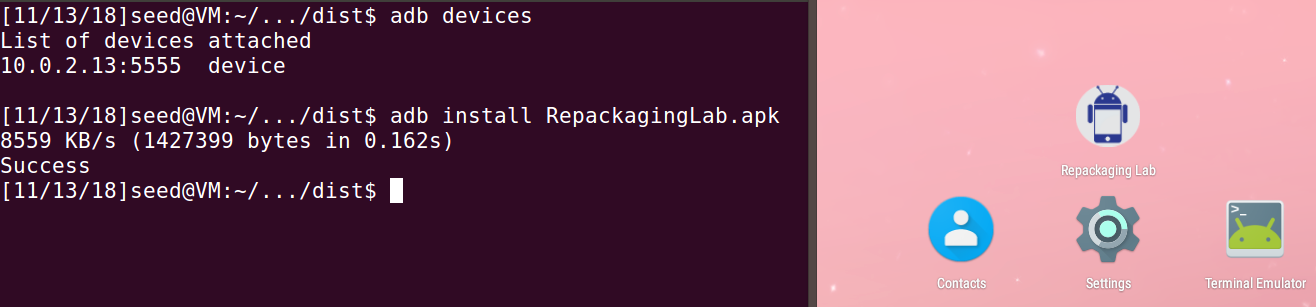


**Task 5: Install the Repackaged App and Trigger the Malicious Code:**

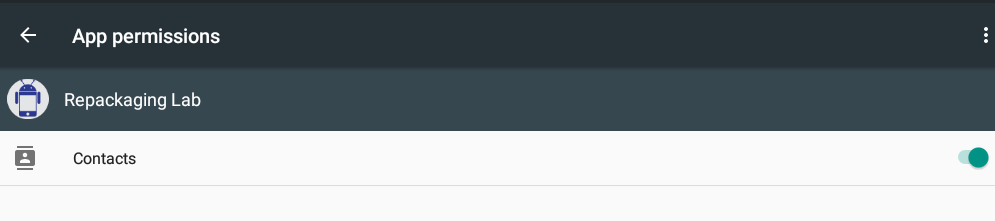
* We first uninstall the previously installed app:



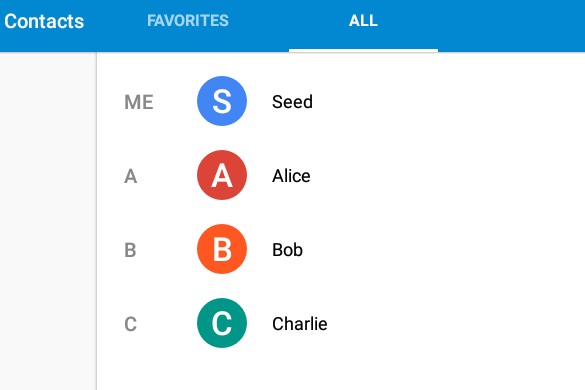
* Then we install our app with malicious code:



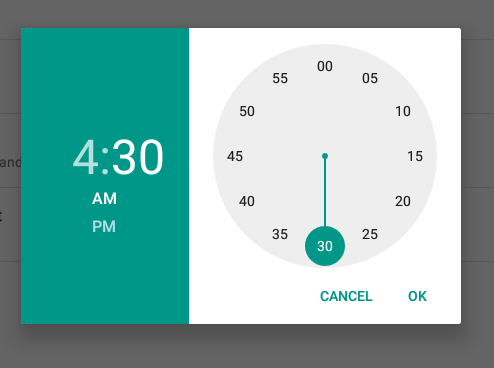
* Giving the contact permissions for the app:

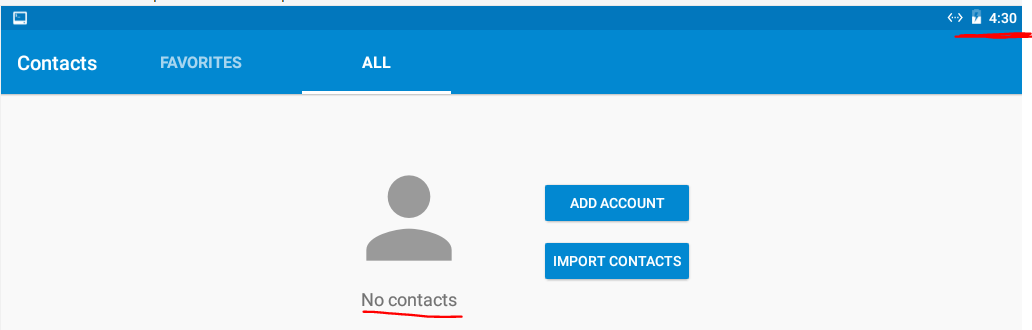


* We add a few contacts:



* We change the time and check the contacts:

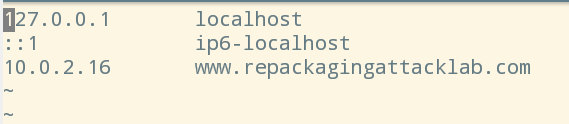




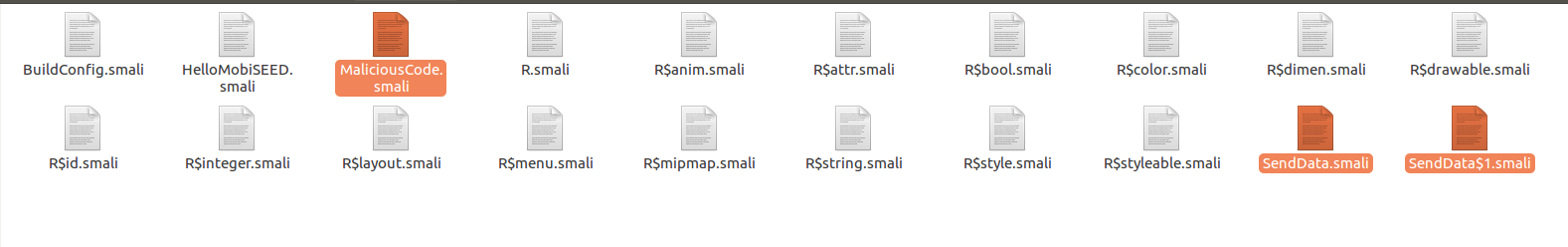
* We can see that the contacts have been erased.
* Changing the time will trigger our malicious code and erase all the contacts.

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

* First we add an entry to the /etc/hosts file in order to map the hostname, [www.repackagingattacklab.com](http://www.repackagingattacklab.com) to the Ubuntu VM’s IP address.



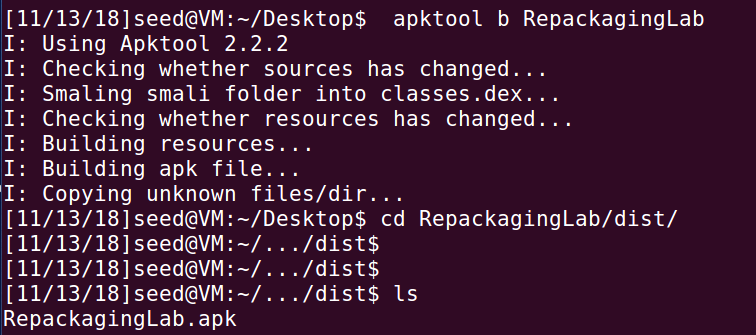
* Placing the 3 smali files in smali/com/mobiseed/repackaging folder of the unpacked application.

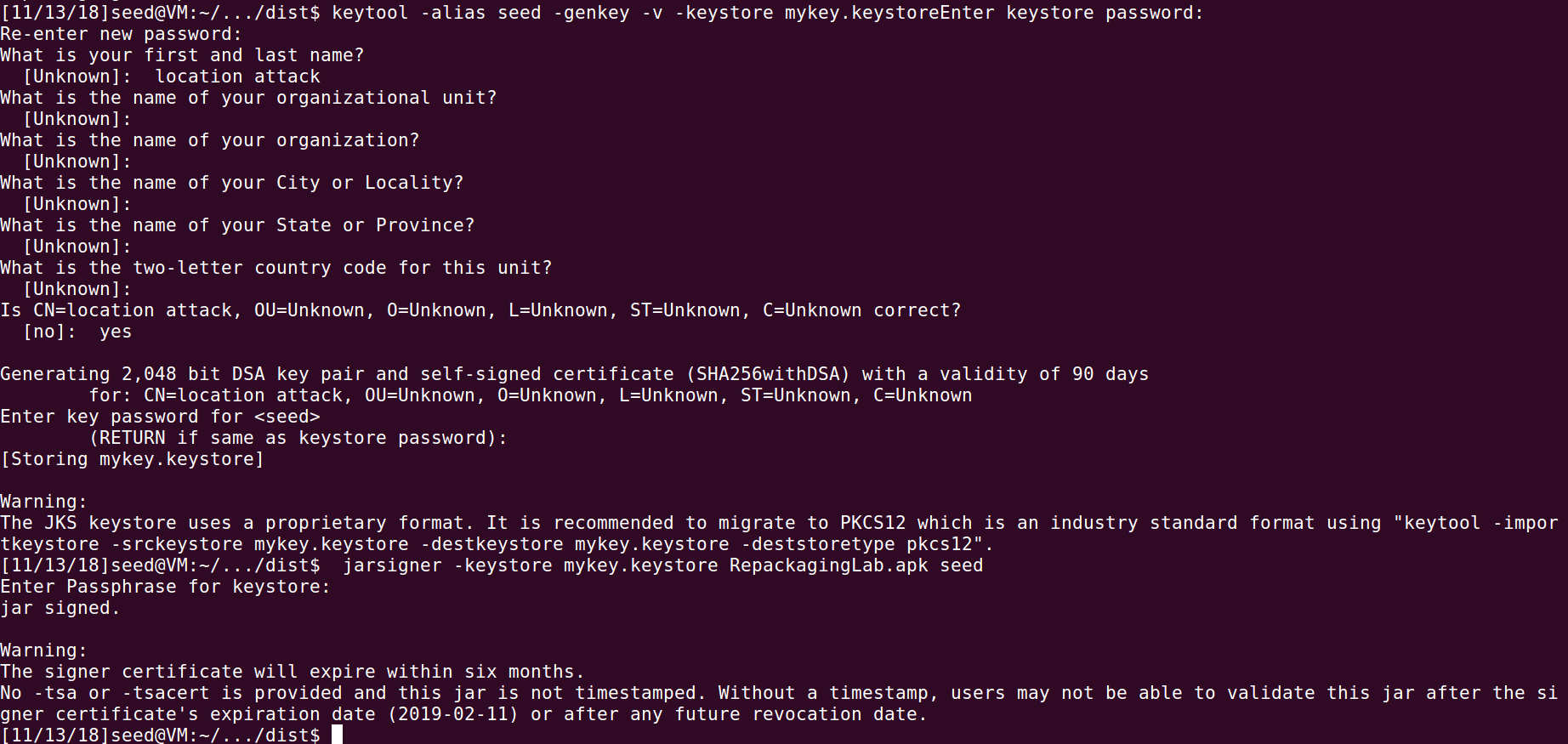


* Changing the AndroidManifest.xml so that it requires the location access permission:

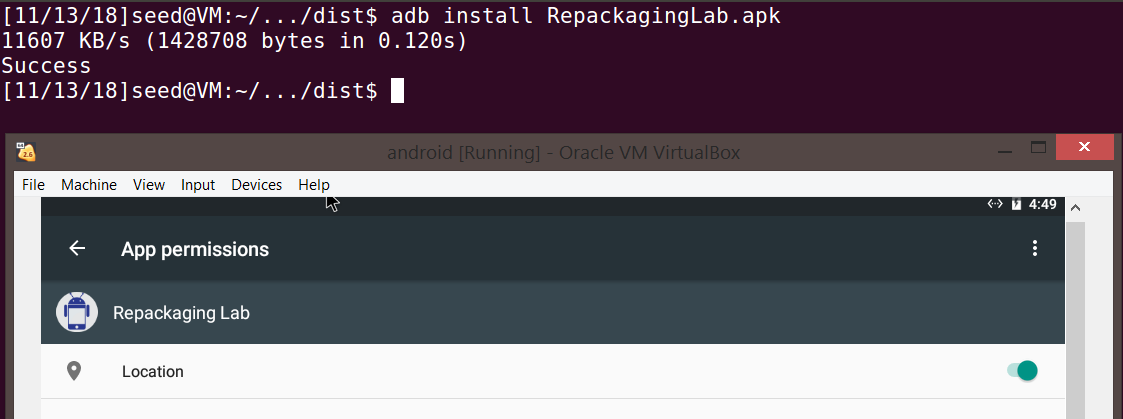


* Then we repack the app using apktool, sign it with the key generated and install it in our Android VM using adb:

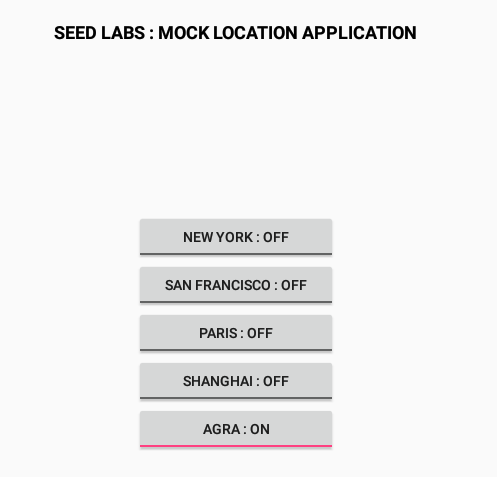




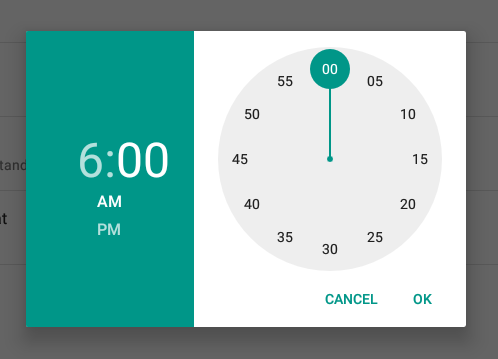
* We also give the permission to access location for the app:



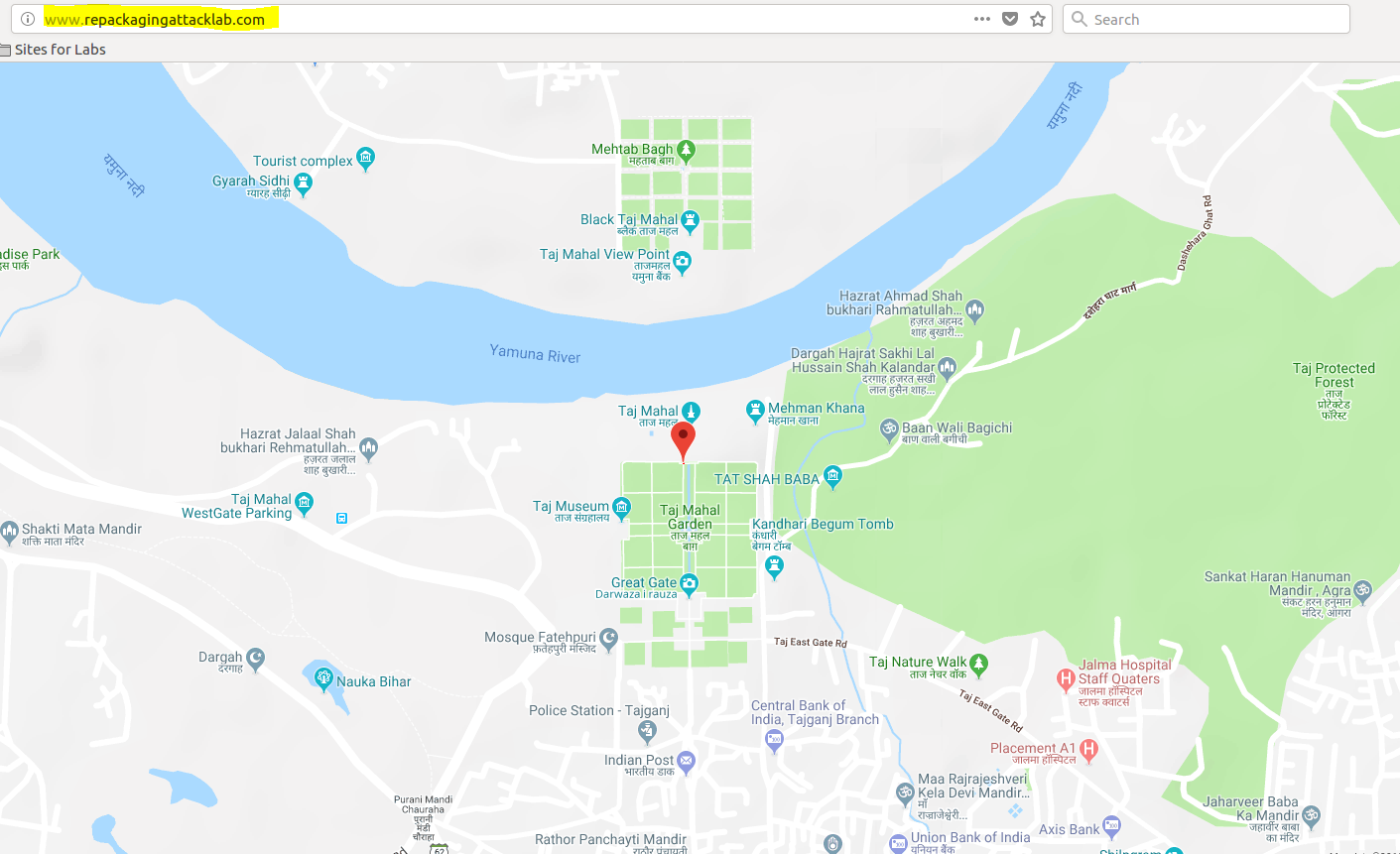
* Using the mock location app installed previously, we choose a location:



* Changing the time will trigger our malicious code to run and the location details is sent to the server.



* Visiting the website, we can see the location the android user is in:



* Changing the location and reloading the page, we can see that the location of the user is updated:

