Tanmay Fadnavis

SUID: 971141760

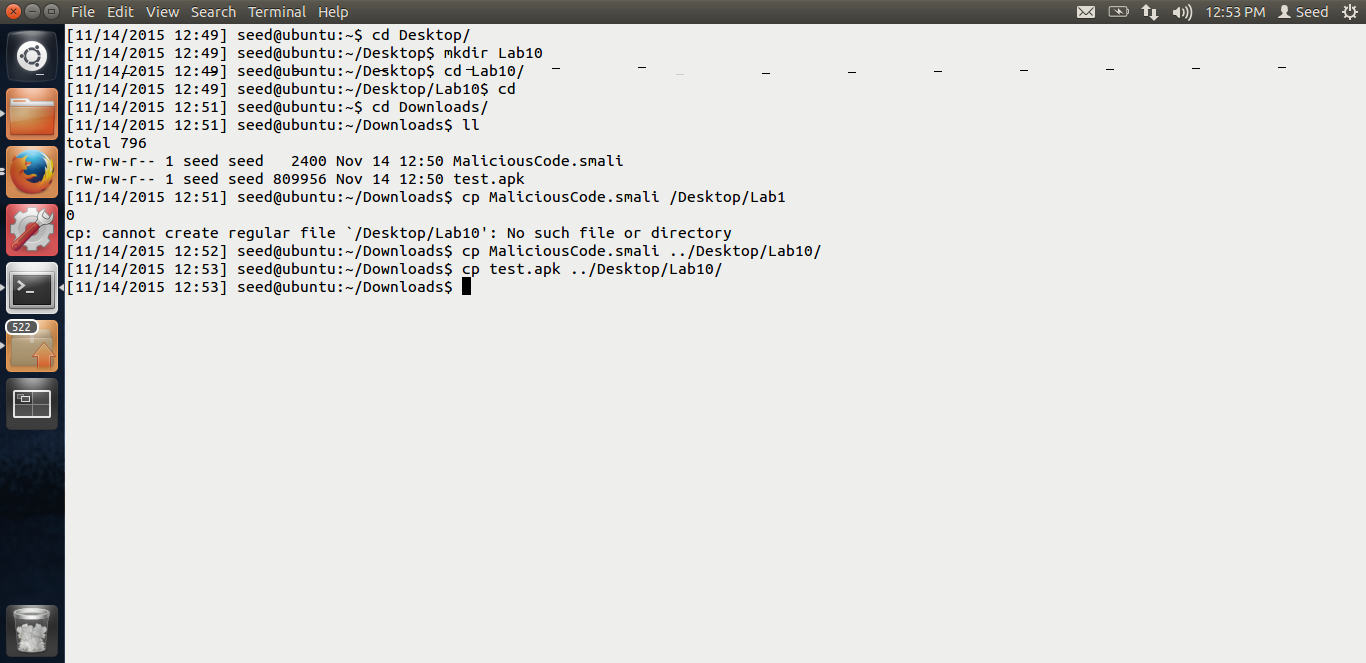
Computer Security

Lab-10

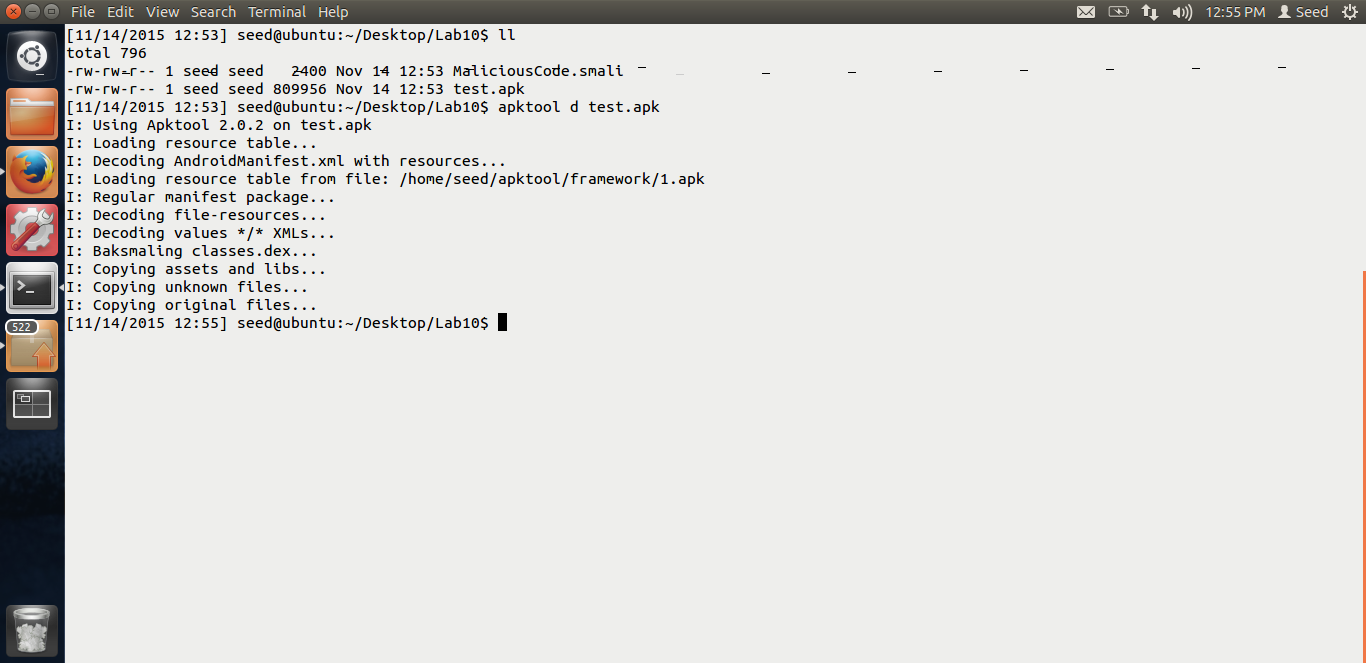
# ANDROID REPACKAGING ATTACK LAB

The screen shots for android repackaging attack lab are below.

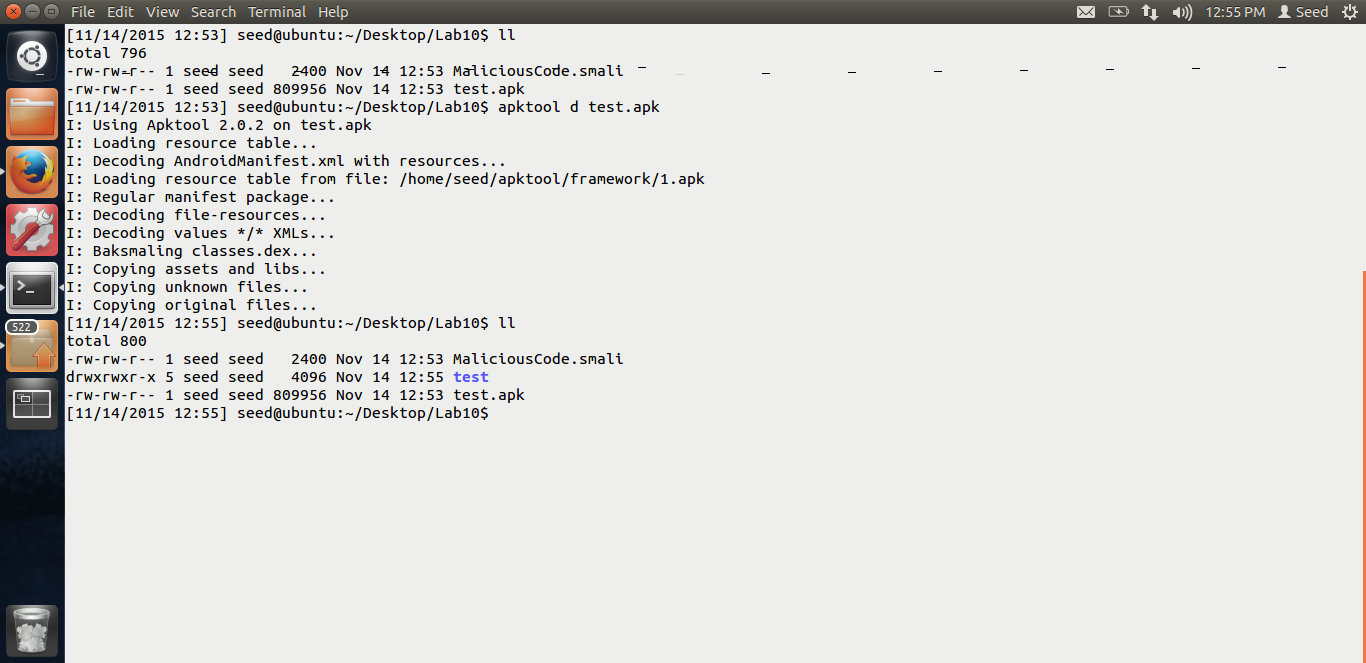
Intially, I have downloaded the android VM and the new Ubuntu VM.



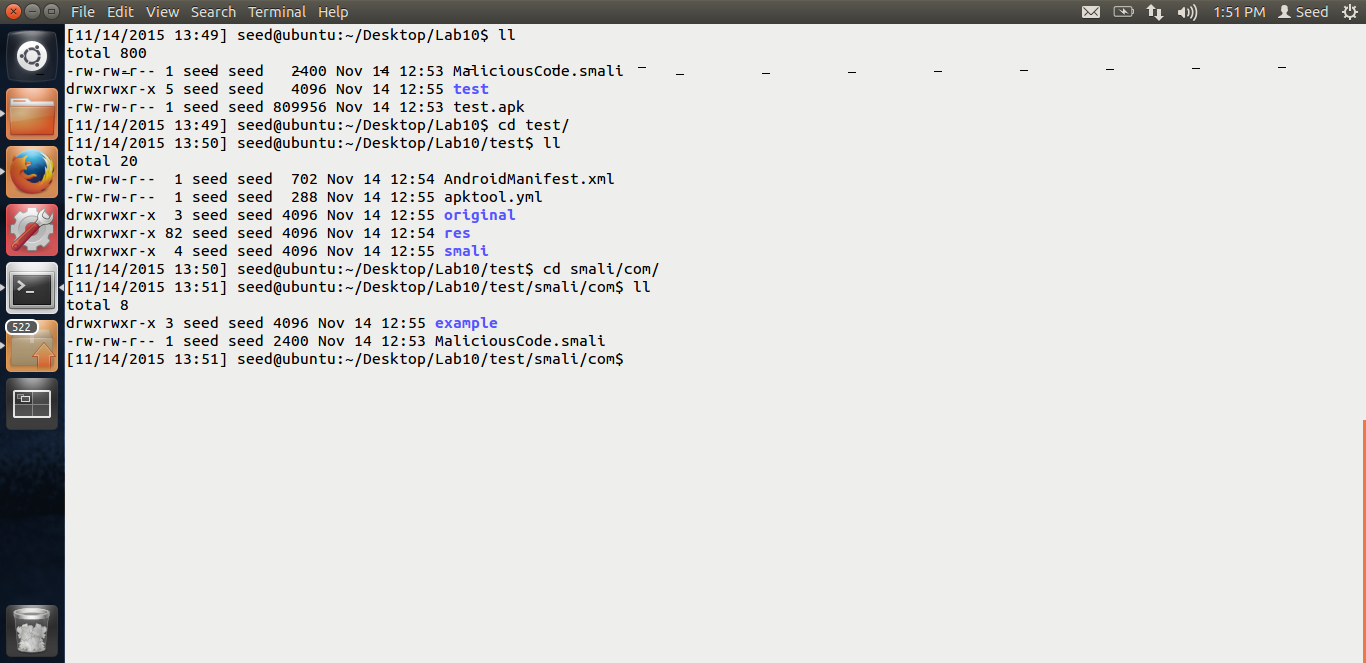
This is the screen shot for the Ubuntu VM. I have downloaded the test.apk and Malicious smali code are we can see in the above screen shot.



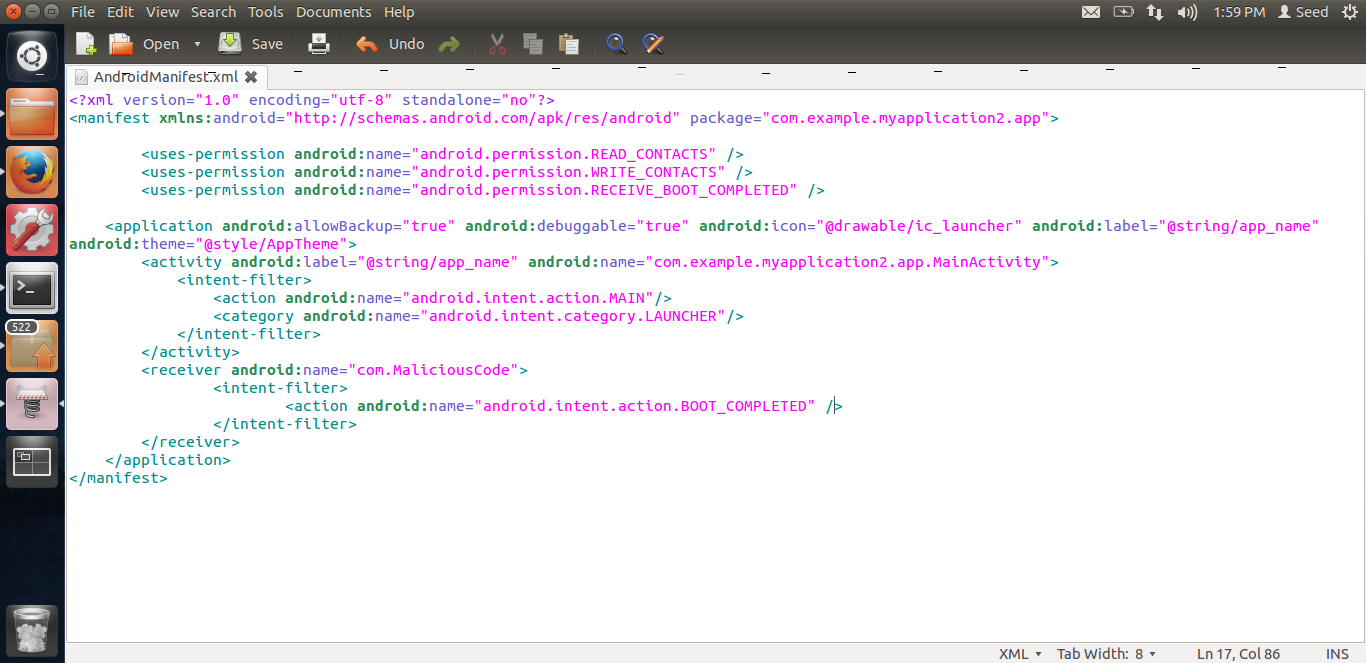
In the above screen shot, you can see that I am decompiling the android app, test.apk, using the command given in the lab, apktool d test.apk.



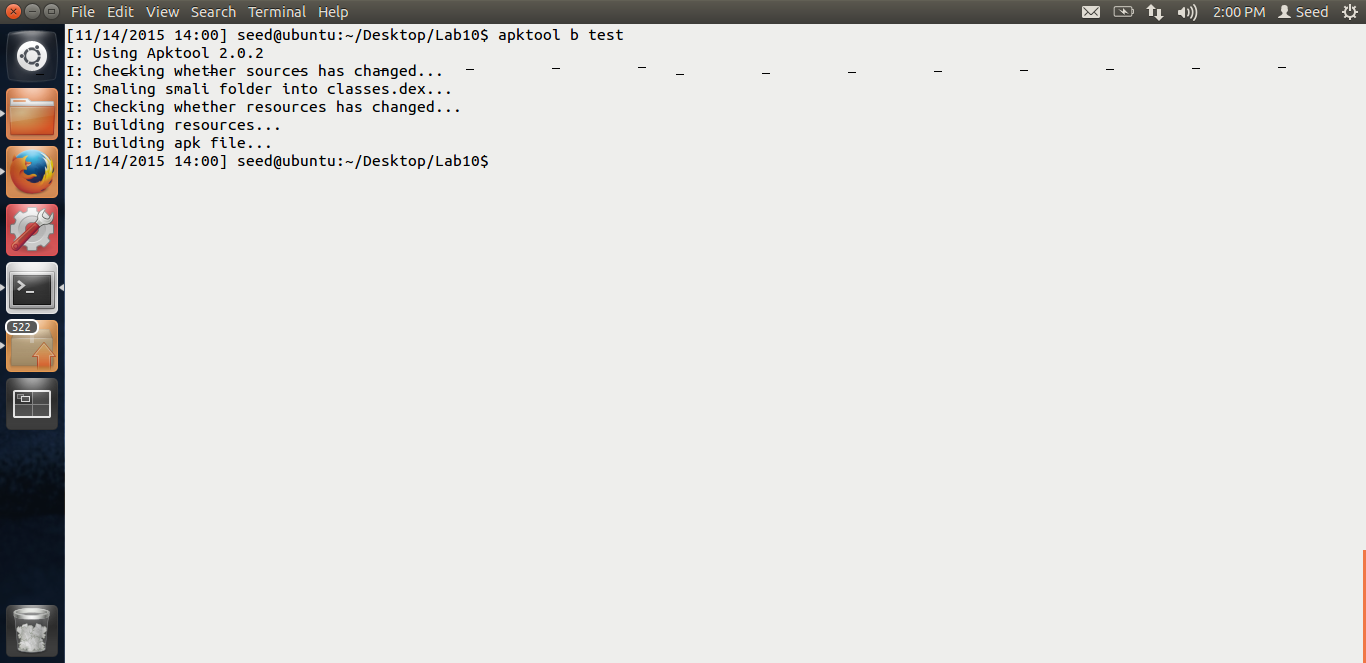
Thus, after decompiling, a folder called “test” has been created as you can see in the above screen shot.



In the above screen shot, you can see that, I have put the malicious smali code in the smali/com folder. “MaliciousCode.smali”. Now, I will make the required changes in the AndroidManifest.xml files.

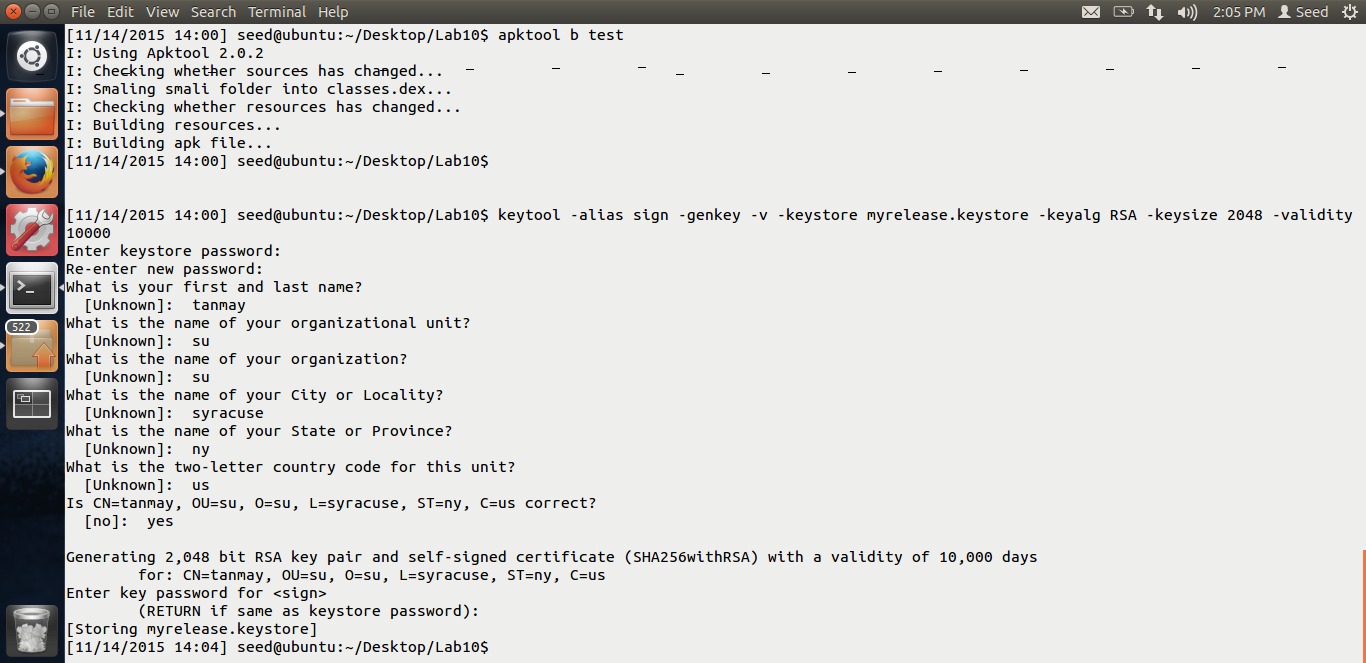


Above is the screen shot for the code I have added in the AndroidManifest.xml file. The code has been given by Dr. Du. I have added the permissions for the application to read and write the contacts and receive the Boot Complete event. Also, there is a receiver which will listen for the BOOT\_COMPLETE event and call our malicious code which is in com.Malicious code after the phone has been BOOTED.

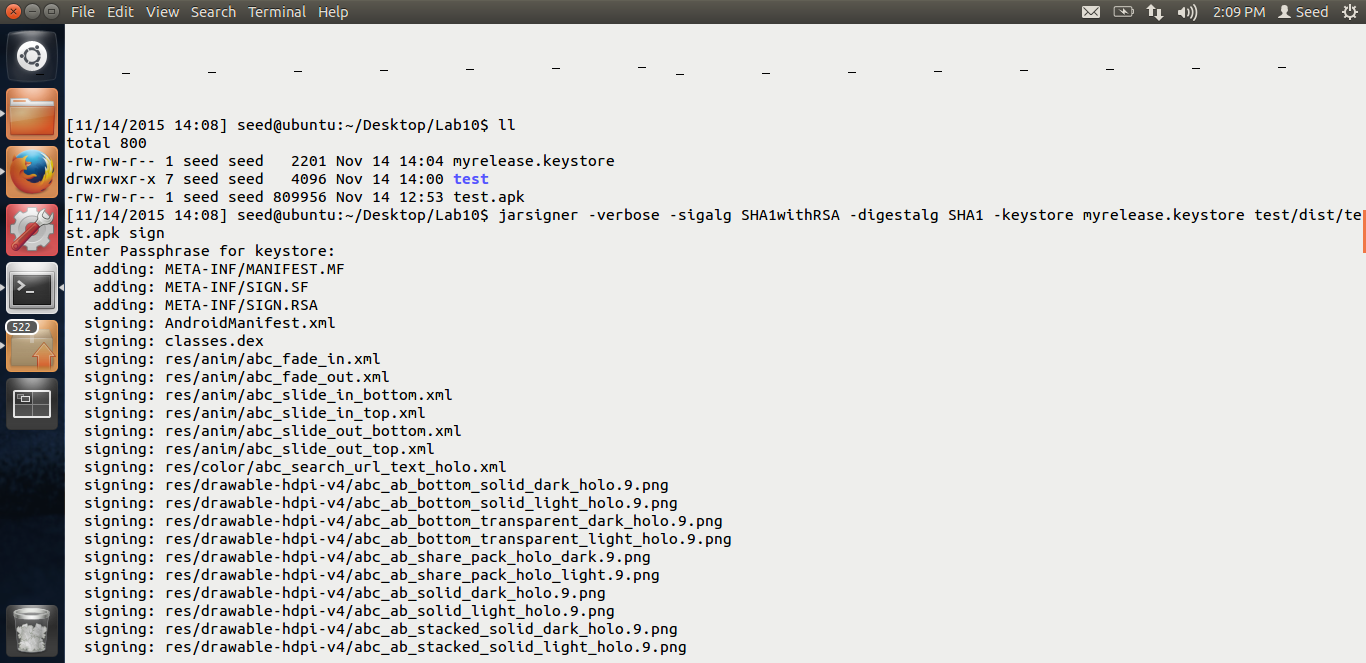


In the above screen shot, we can see that, I am repackaging the application with these changes which contain the malicious code.

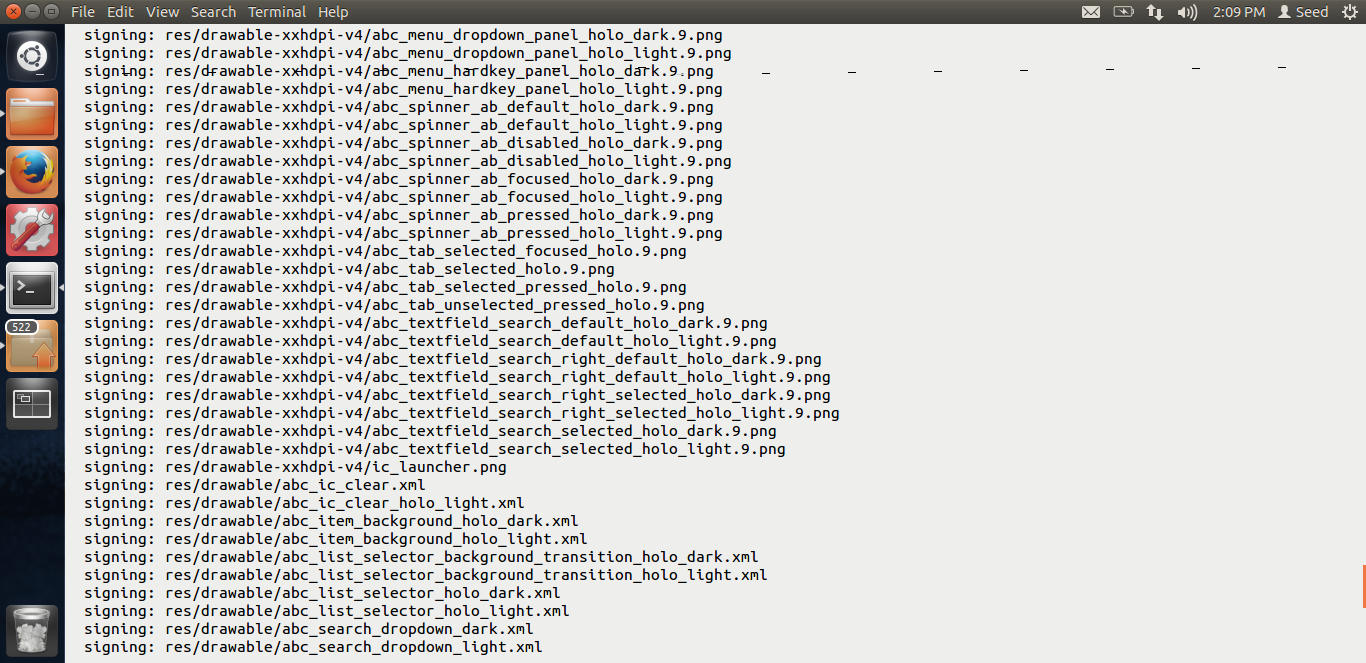
The command used is apktool b test. Test is the application folder. Next we need to sign the apk.

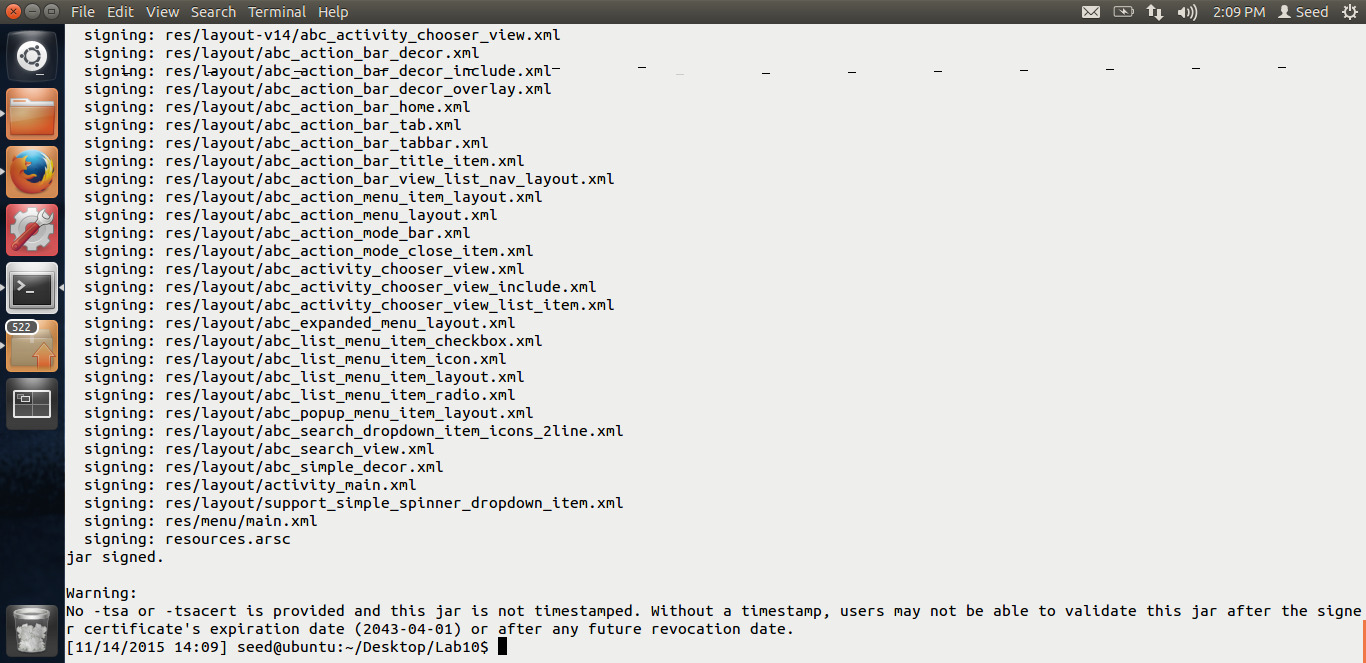


In the above screen shot, we can see that I am generating the private key using the keytool command given in the lab. My alias is sign and the key is myrelease.keystore. Now, let us sign the application using this generated key.



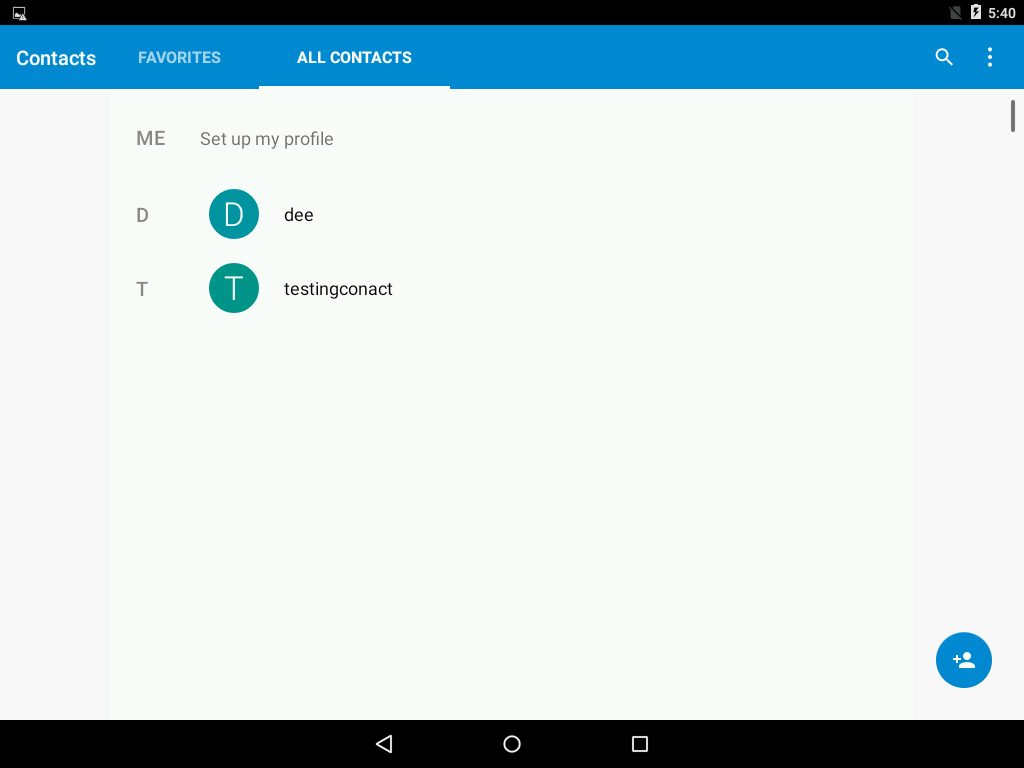
Here, I am using jarsigner as mentioned in the lab to sign the application. Important thing to note is, the path of the apk is test/dist/test.apk The reason is, the newly recompiled apk with the malicious code is in the dist folder.



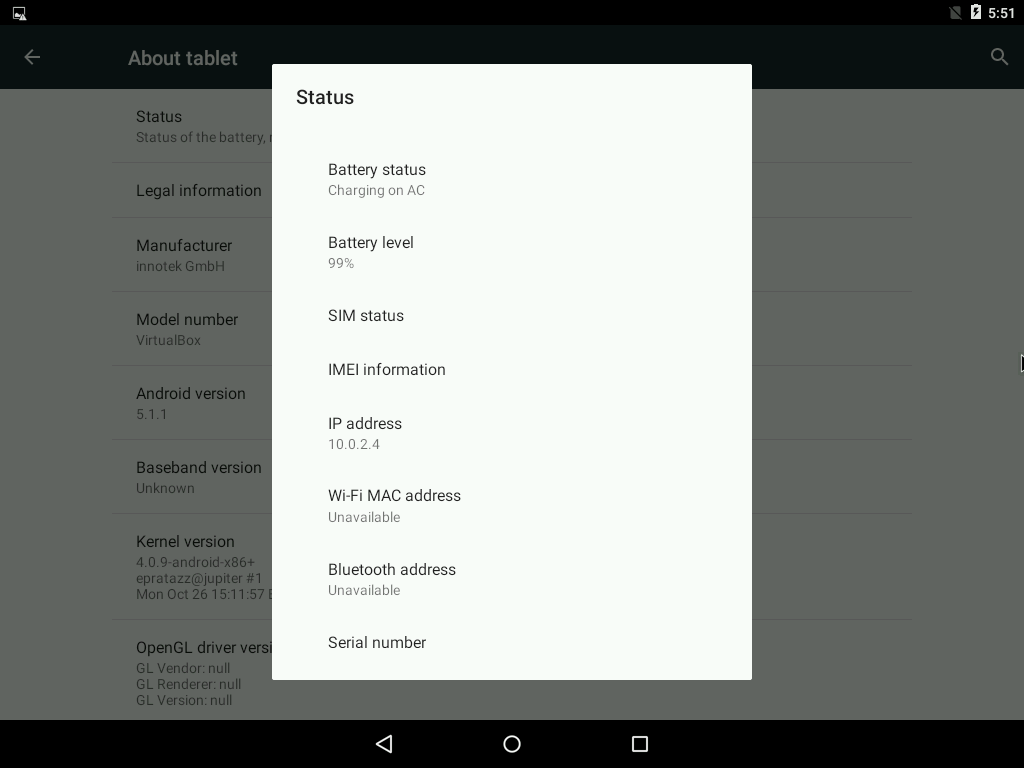


Thus, from the above screen shots, we can see that the new application with the malicious code has been signed and is ready to be distributed.

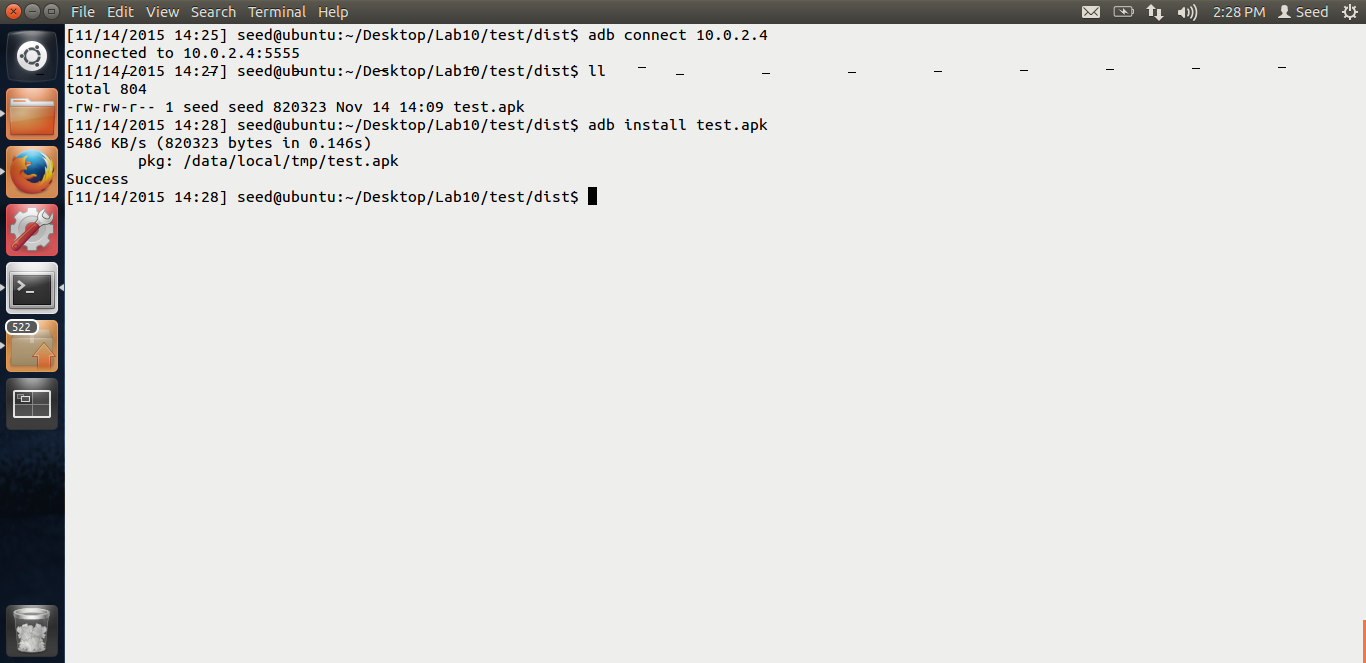
Now, let us install this malicious application on our android vm and see if the attack works.



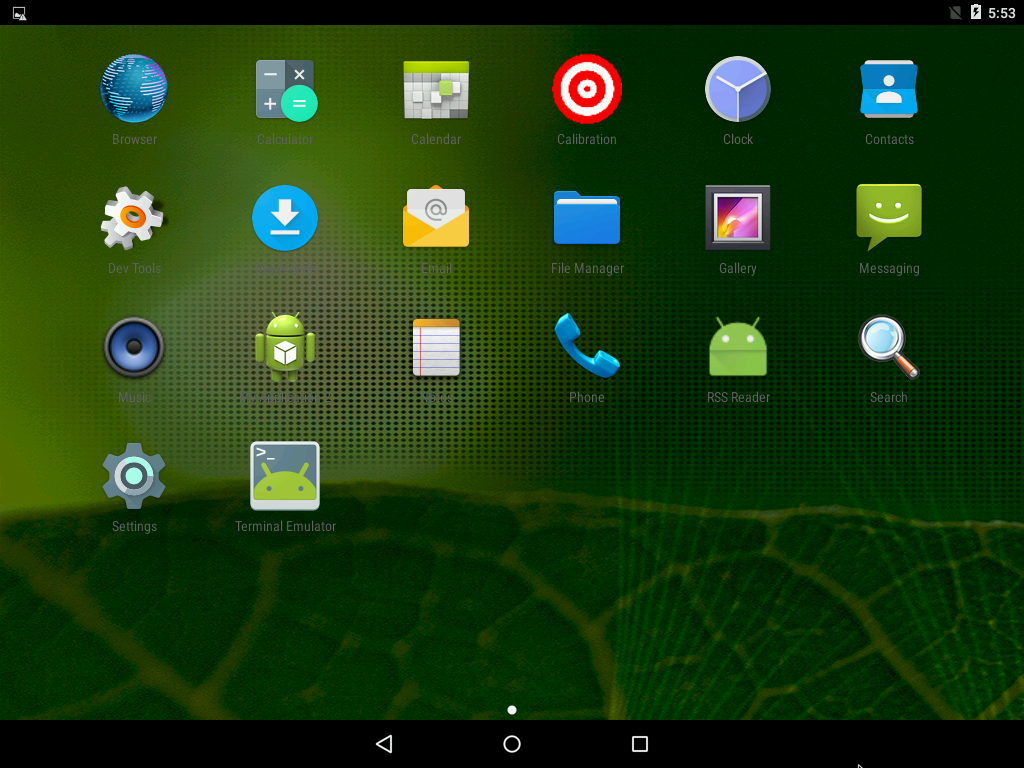
In the above screen shot, which is of the android VM, you can see, I have added a testing contact, dee contact was already installed on the phone.



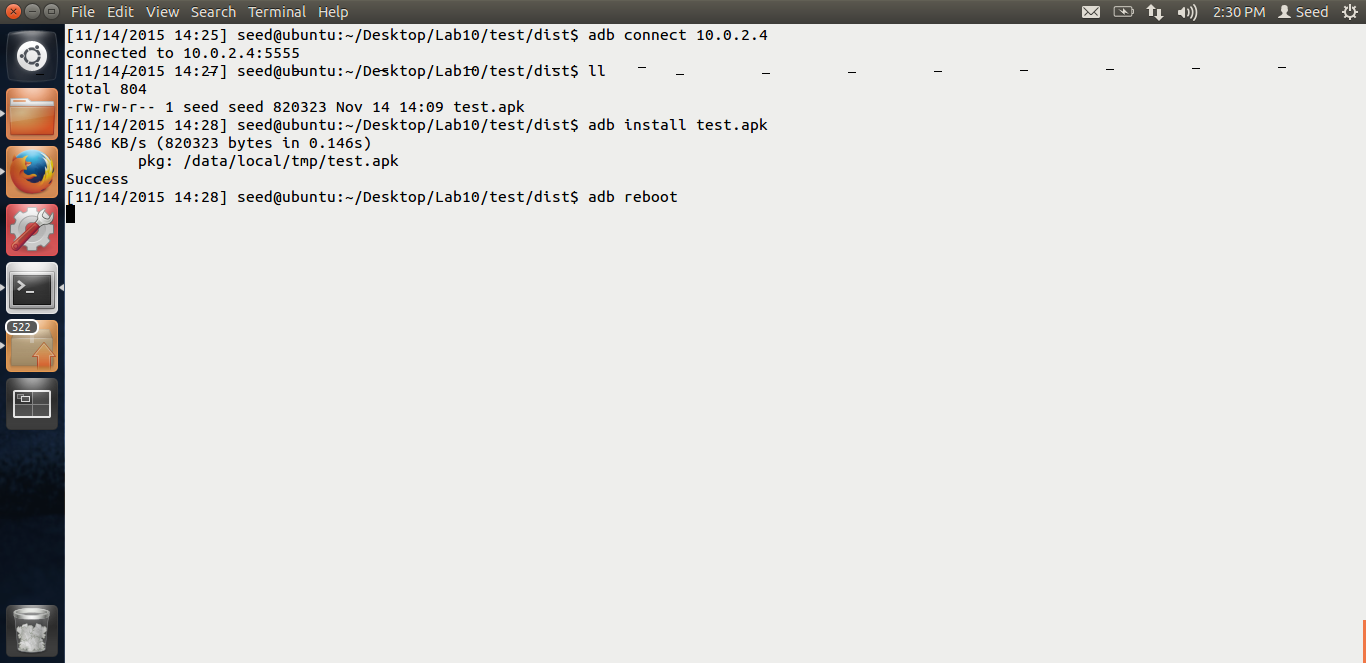
Now, to connect to the android VM, we need the IP address. Above is the IP address for the same. Let us connect to vm and see what happens.



In the above screen shot, you can see that I have connected to the android vm using the adb connect. Also, I have installed the application on our android, using the adb install test.apk



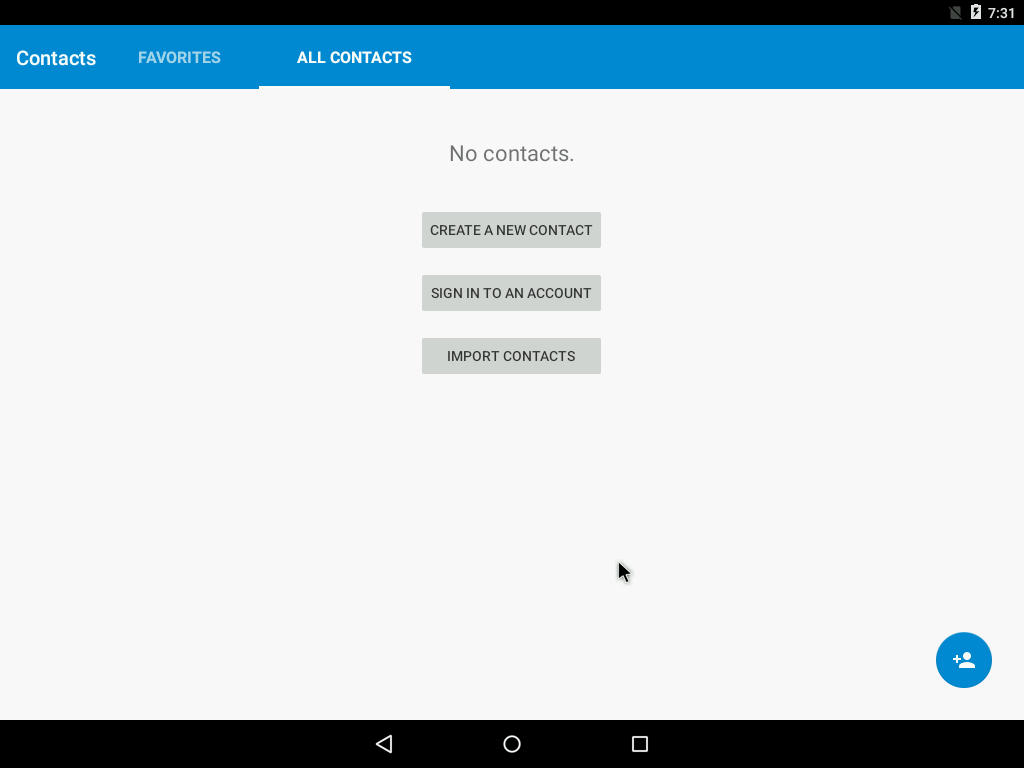
In the above screen shot, the application we can see as installed.



Now, we have to reboot the android vm, because only after the BOOT event is completed, our malicious code will run and the attack will be successful. Thus, I am rebooting the android using the adb reboot command.



As you can see the android is rebooting. Now after the reboot, let us check our contacts and see whether the attack was successful.



As soon as we click on the contacts, you can see that the 2 contacts are gone. No contacts are present. Thus, our attack was successful. Thus, we were successful in deleting the contacts after the phone was booted and our malicious code did the damage. This shows that it is a big risk to download applications from 3rd party other than Google play because the risk associated with it is too high.

Thus, this is the end of Lab-10.