**CSCE 548 Project 3**

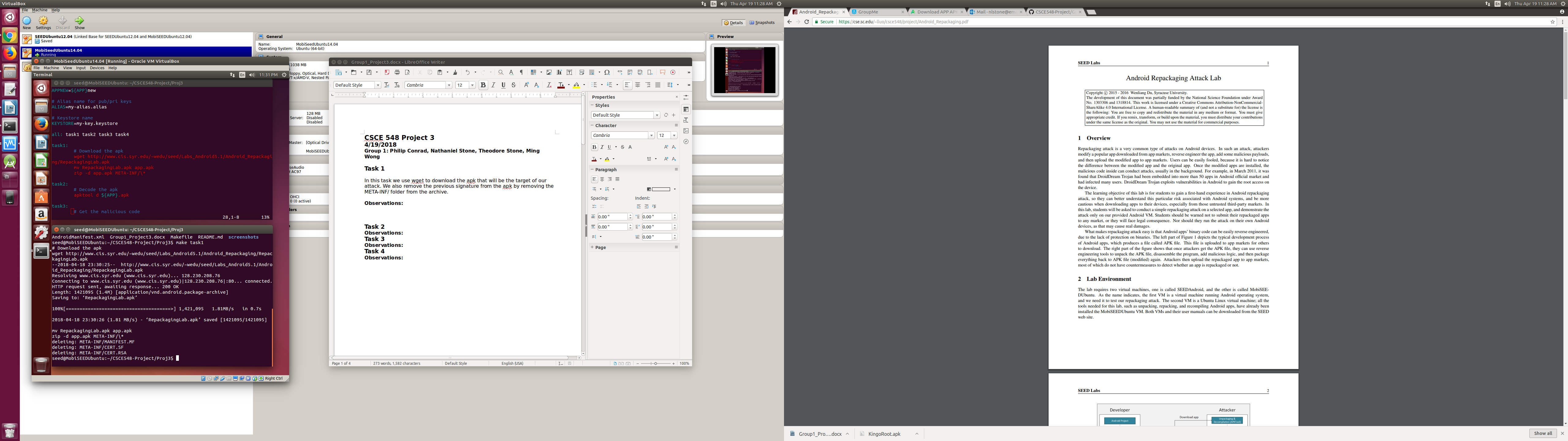
**4/19/2018**

**Group 1: Philip Conrad, Nathaniel Stone, Theodore Stone, Ming Wong**

**Task 1**

In this task we use wget to download the apk that will be the target of our attack. We also remove the previous signature from the apk by removing the META-INF/ folder from the archive.

**Observations:**

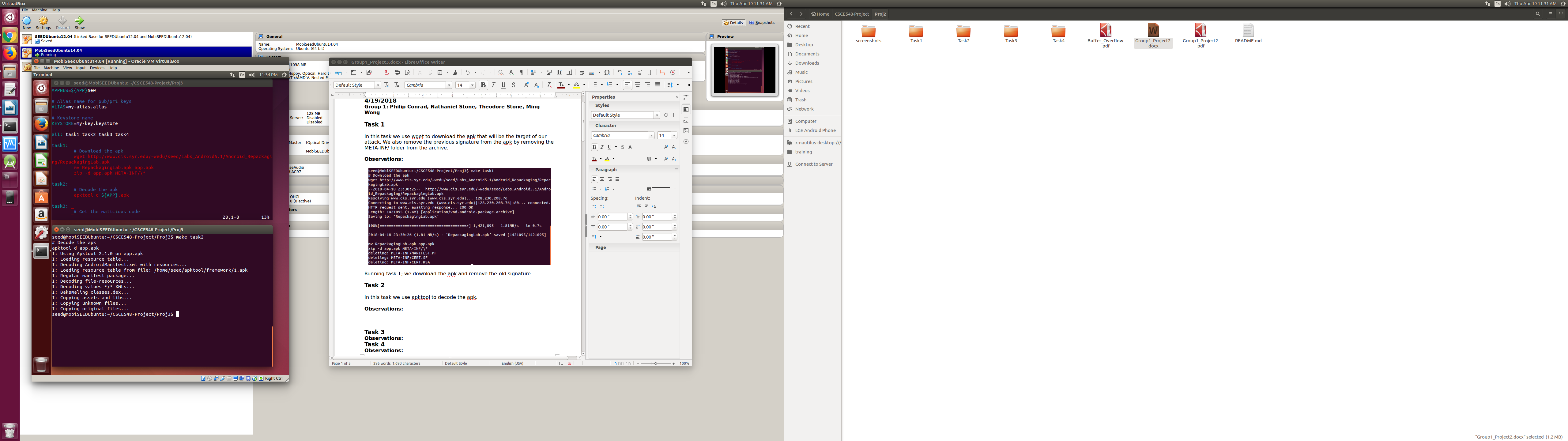


Running task 1; we download the apk and remove the old signature.

**Task 2**

In this task we use apktool to decode the apk.

**Observations:**



Using apktool to decode the apk.

**Task 3**

**Observations:**

**Task 4**

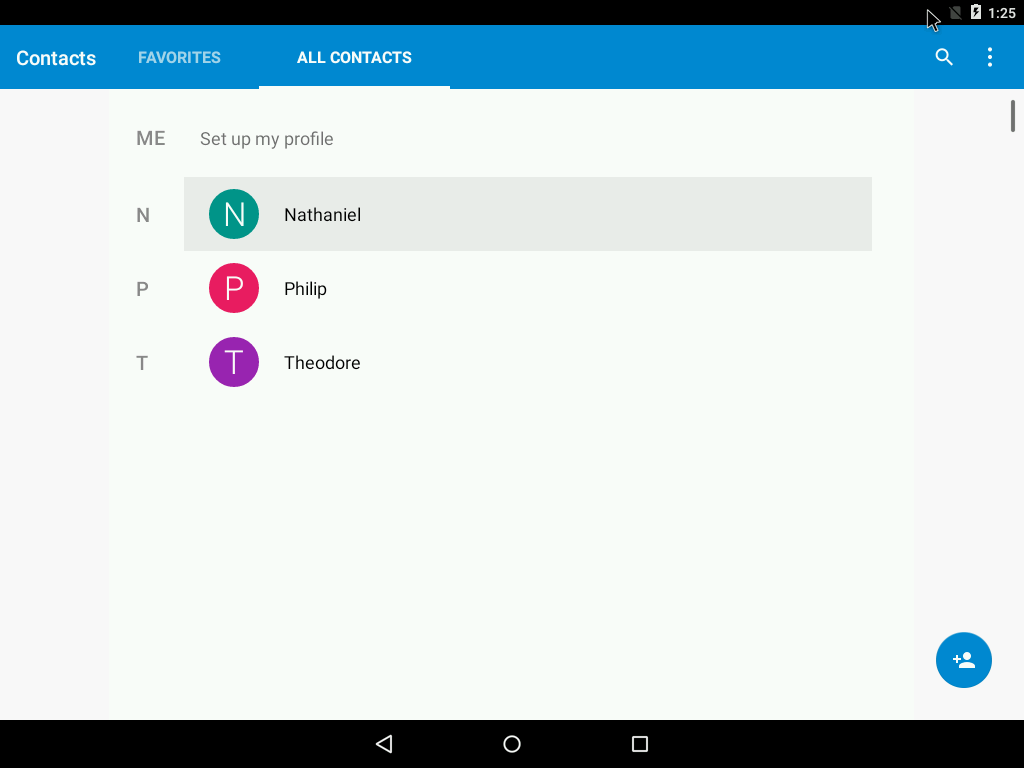
**Observations:**

**Task 5**

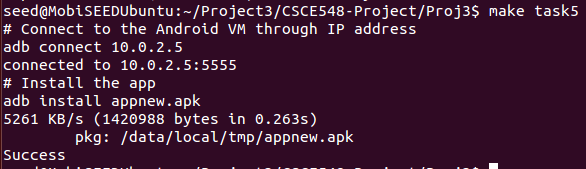
The goal of this task is to install the malicious app onto the android device. We first determine the IP address of the android by typing *netfcg* on the android terminal. After that, we connect our Ubuntu machine to our android emulator to install our newly modified app.

**Observations:**

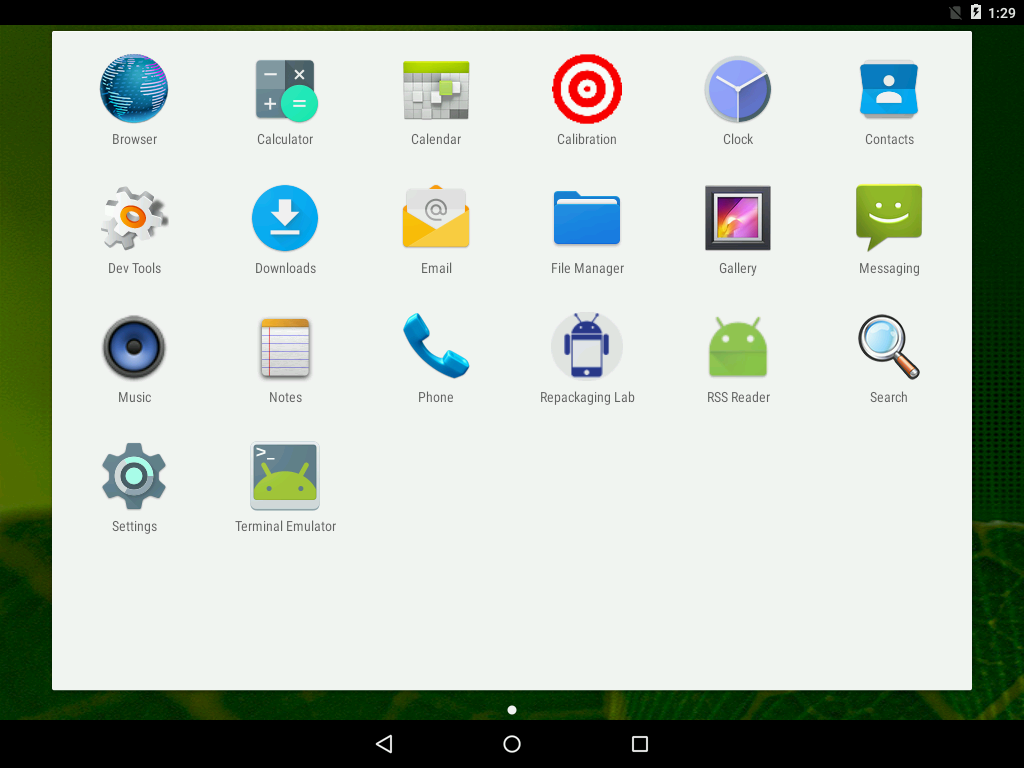
Before we install the app, there are three contacts.



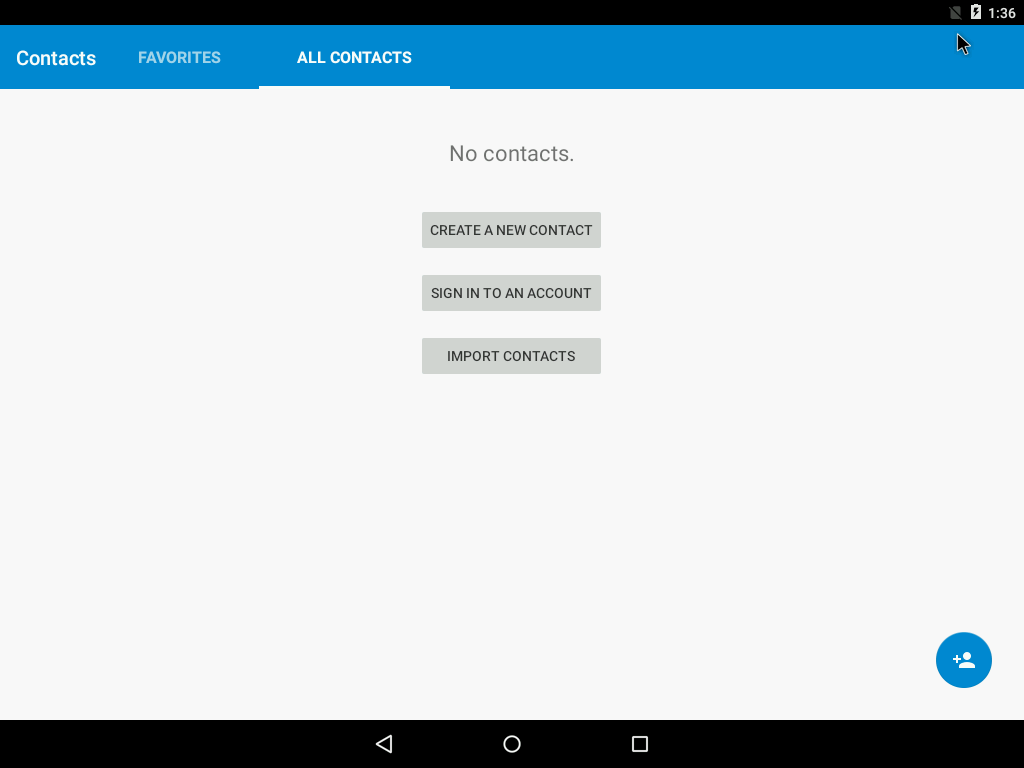
We use these commands to perform our app installation.



We observe that our appnew.apk is installed onto the android device. It still uses the original name of the app, which is Repacking Lab.



When we launch the Repackaging Lab once and restart the android device, we notice all our contacts have been obliterated by our successful repackaging attack.



**Lab Questions**

1. **Why is the repackaging attack not much a risk in iOS devices?**

TODO

1. **If you were Google, what decisions you would make to reduce the attacking chances of repackaging attacks?**
2. **Third-party markets are considered as the major source of repackaged applications. Do you think that using the official Google Play Store only can totally keep you away from the attacks? Why or why not?**
3. **In real life, if you had to download applications from untrusted source, what would you do to ensure the security of your device?**