Lab #3
Android Repackaging Lab

Name : Adithya Karthikeyan
SJSU ID : 011991941

1) First we download the **"RepackagingLab.apk"** file and then disassemble the apk file with the apktool d command as shown in Figure 1. We disassemble the file because the file is in a dex format and modifying it in that format is vey difficult. We convert it to something that is readable by humans.

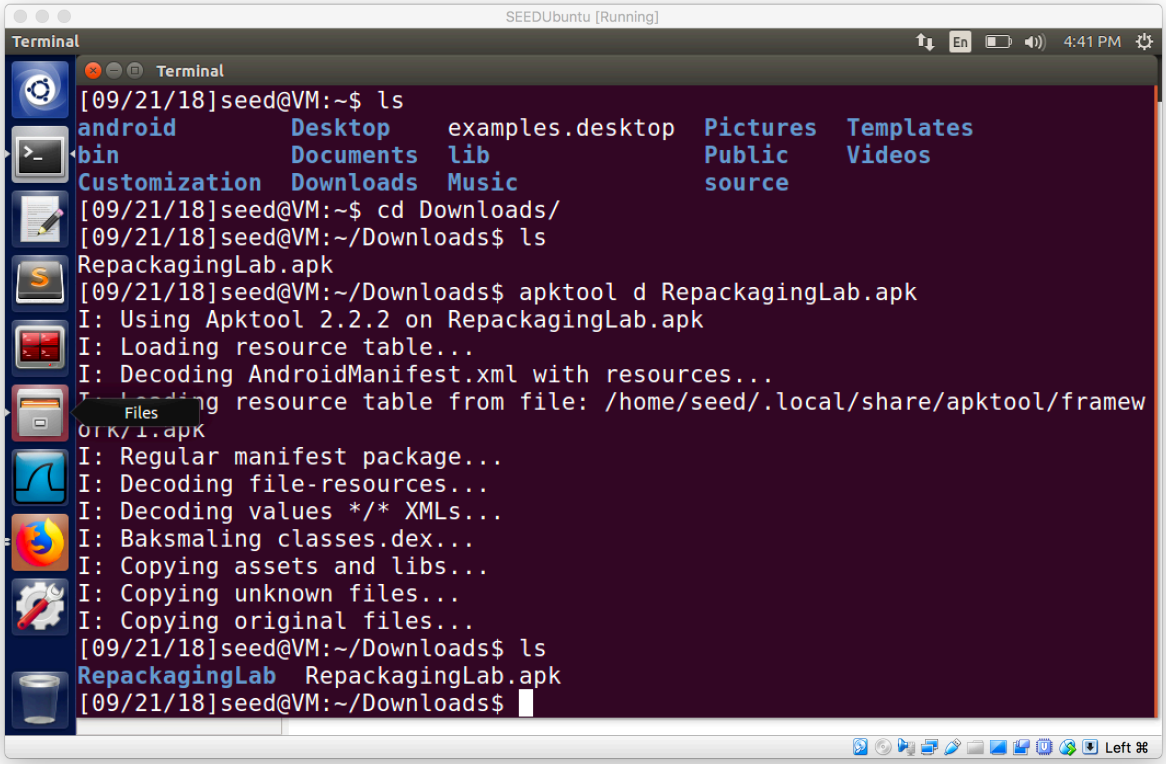


Figure 1

2) Next, we modify the xml file to give it the necessary permissions for our attack to work. The xml file is shown in the below figure.

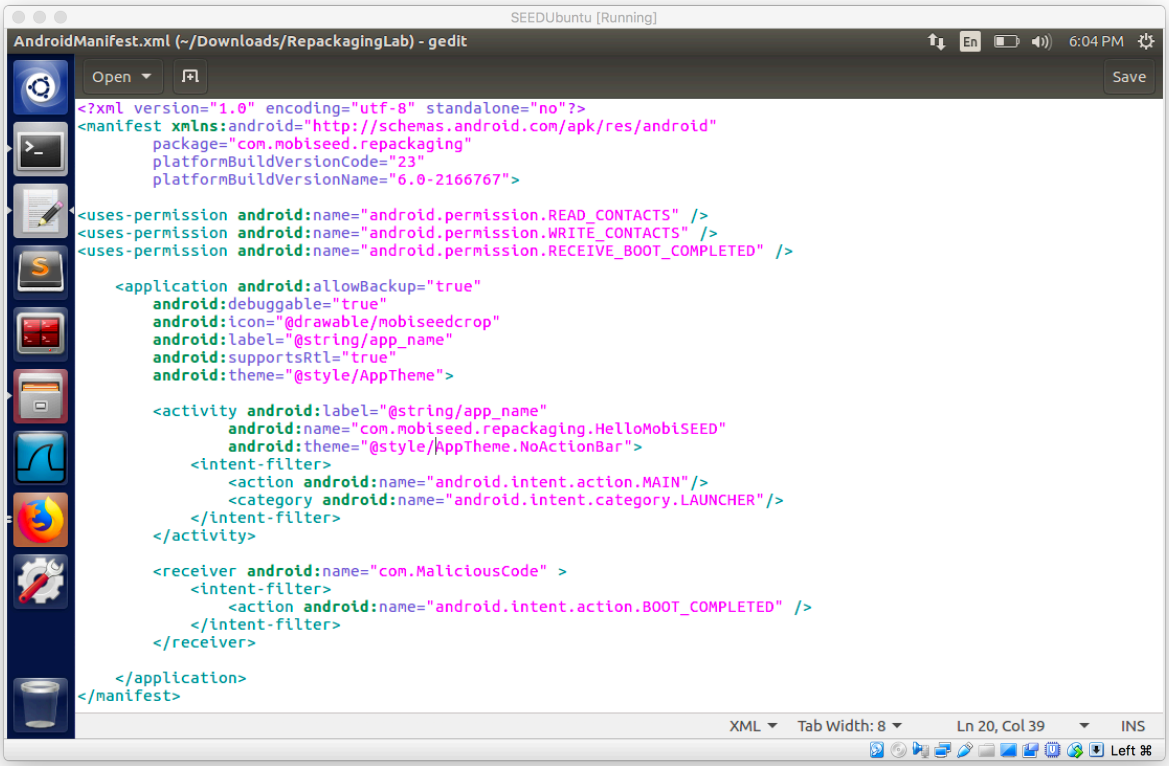


Figure 2

3) We also download the smali code and place it in the com folder of the disassembled apk file. Now, we repack the Android app with the malicious code using the apktool b command. Once the repackaging is done, the apk file is placed in the **dist** file. Below is the attached screenshot.

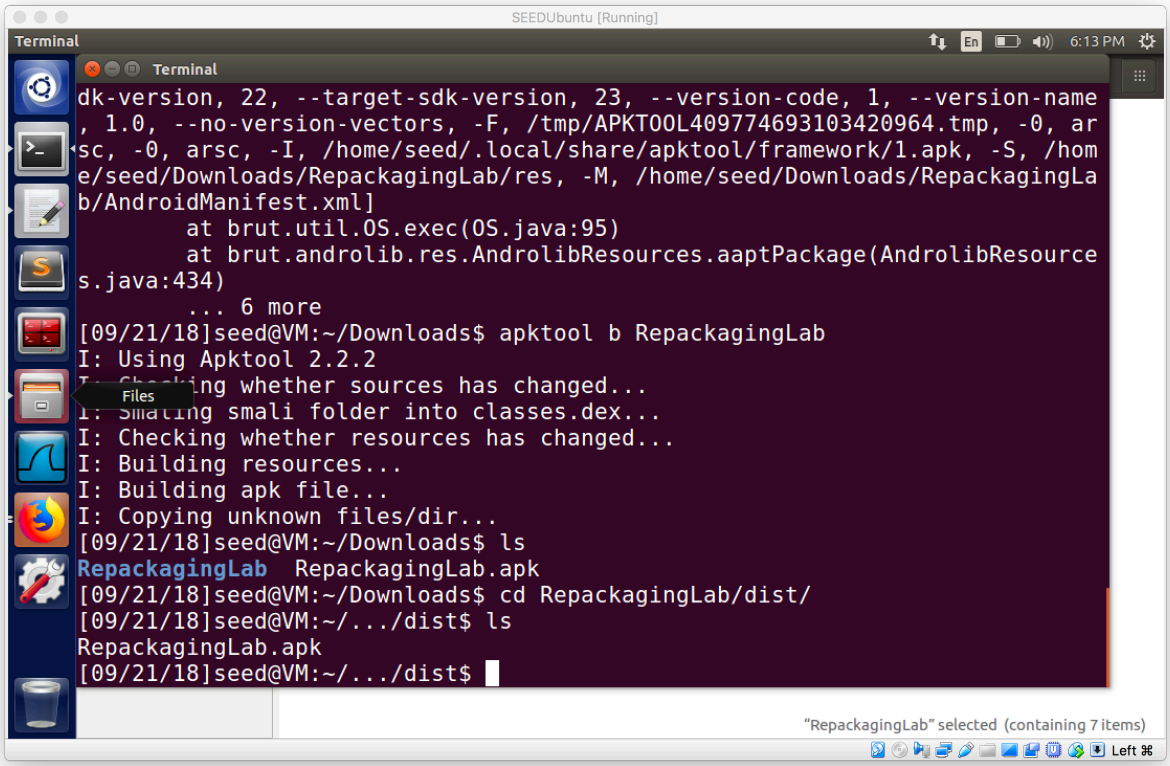


Figure 3

4) Next, we generate the public key, private key and digital certificate using the command below. Android requires a public and a private key and **Keytool** is used to generate these. **Jarsigner** is used to sign the certificate.

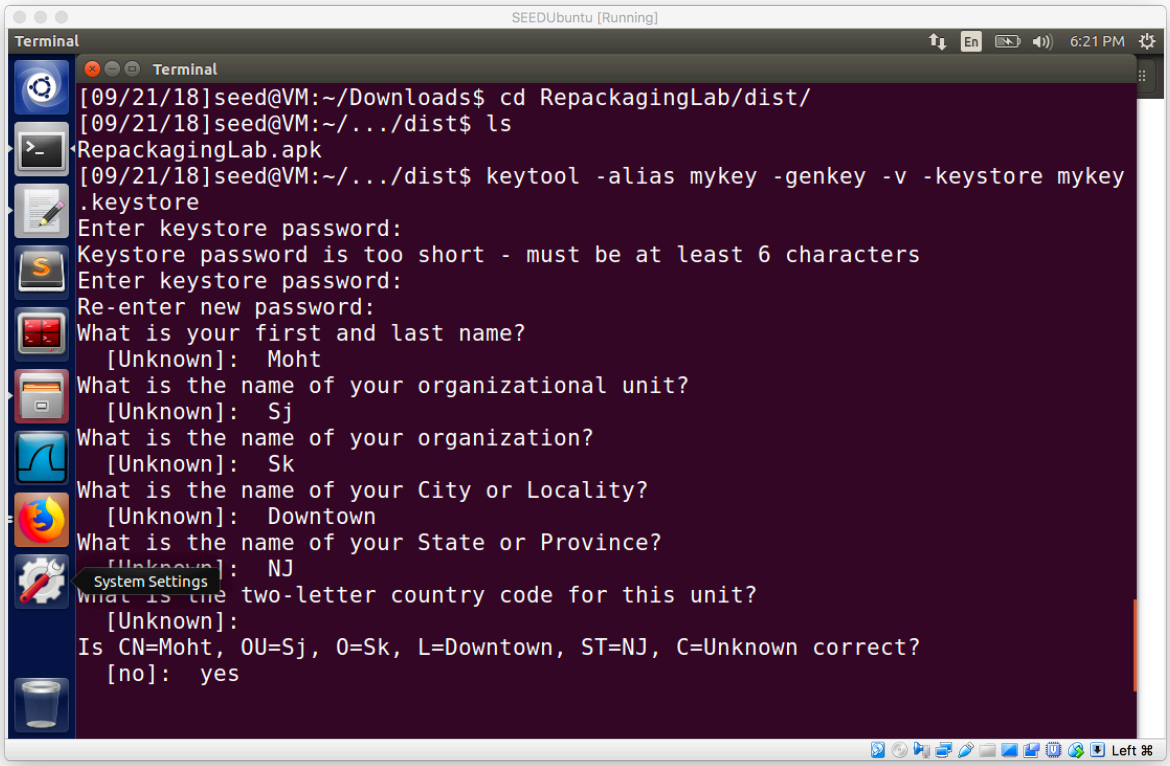

SEEDUbuntu [Running]
Terminal
6:21 PM
Terminal
[09/21/18]seed@VM:~/Downloads$ cd RepackagingLab/dist/
[09/21/18]seed@VM:~/.../dist$ ls
RepackagingLab.apk
[09/21/18]seed@VM:~/.../dist$ keytool -alias mykey -genkey -v -keystore mykey
.keystore
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: Moht
What is the name of your organizational unit?
[Unknown]: Sj
What is the name of your organization?
[Unknown]: Sk
What is the name of your City or Locality?
[Unknown]: Downtown
What is the name of your State or Province?
[Unknown]: NJ
System Settings
What is the two-letter country code for this unit?
[Unknown]:
Is CN=Moht, OU=Sj, O=Sk, L=Downtown, ST=NJ, C=Unknown correct?
[no]: yes
Left ⌘

Figure 4

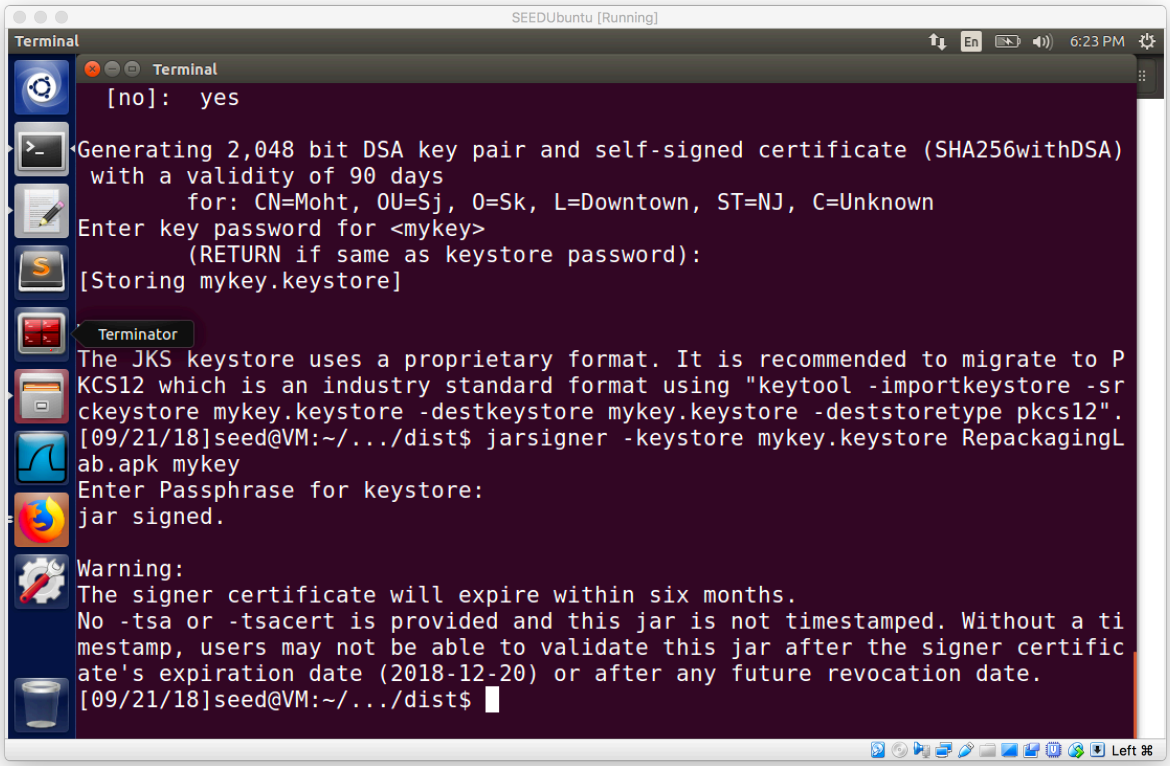
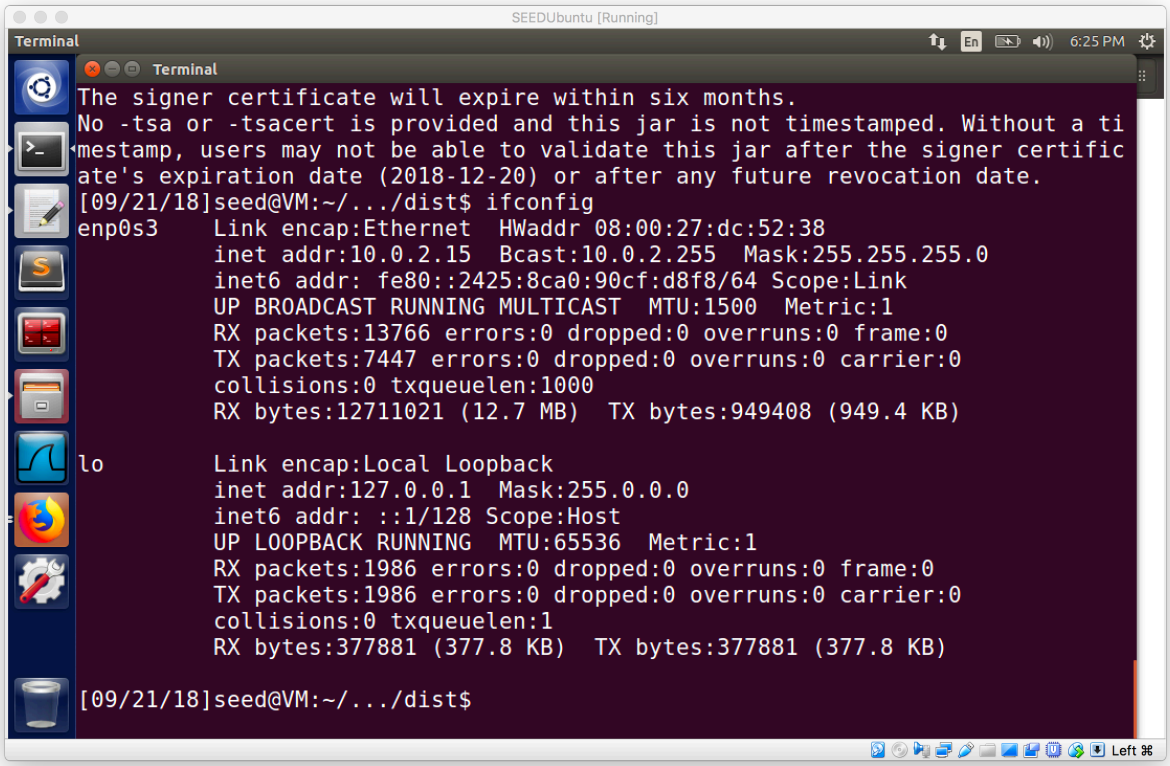
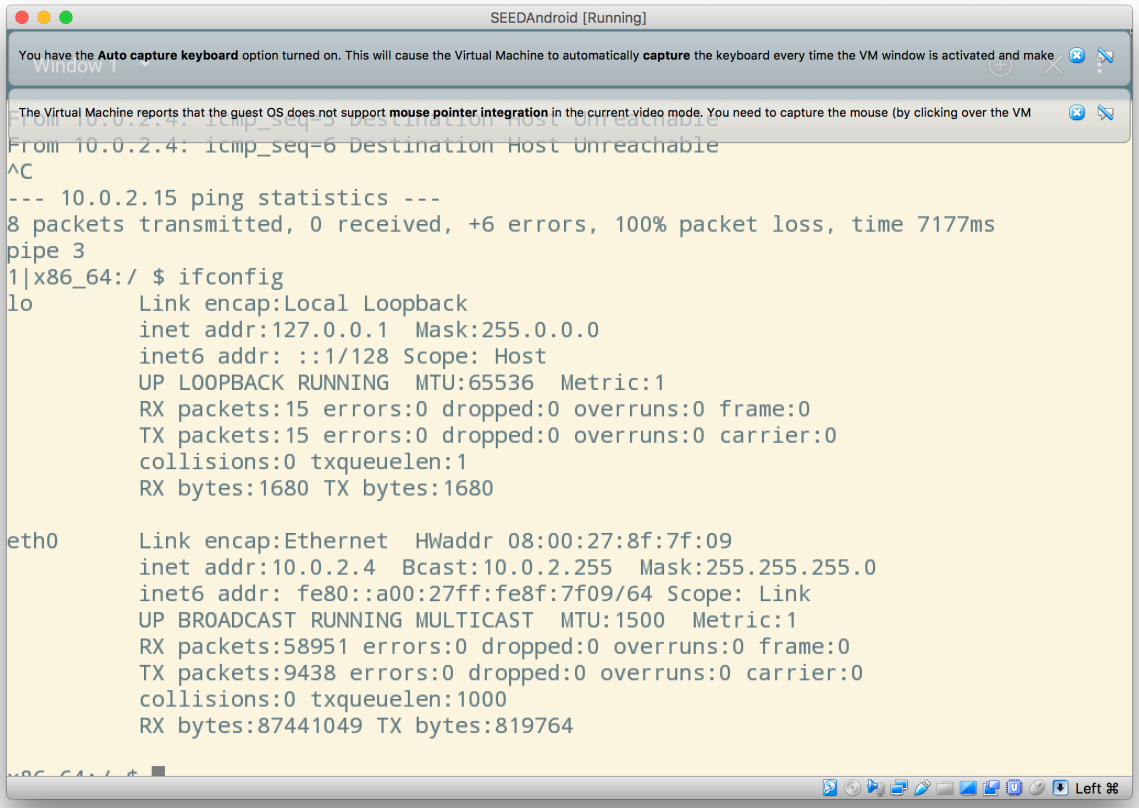
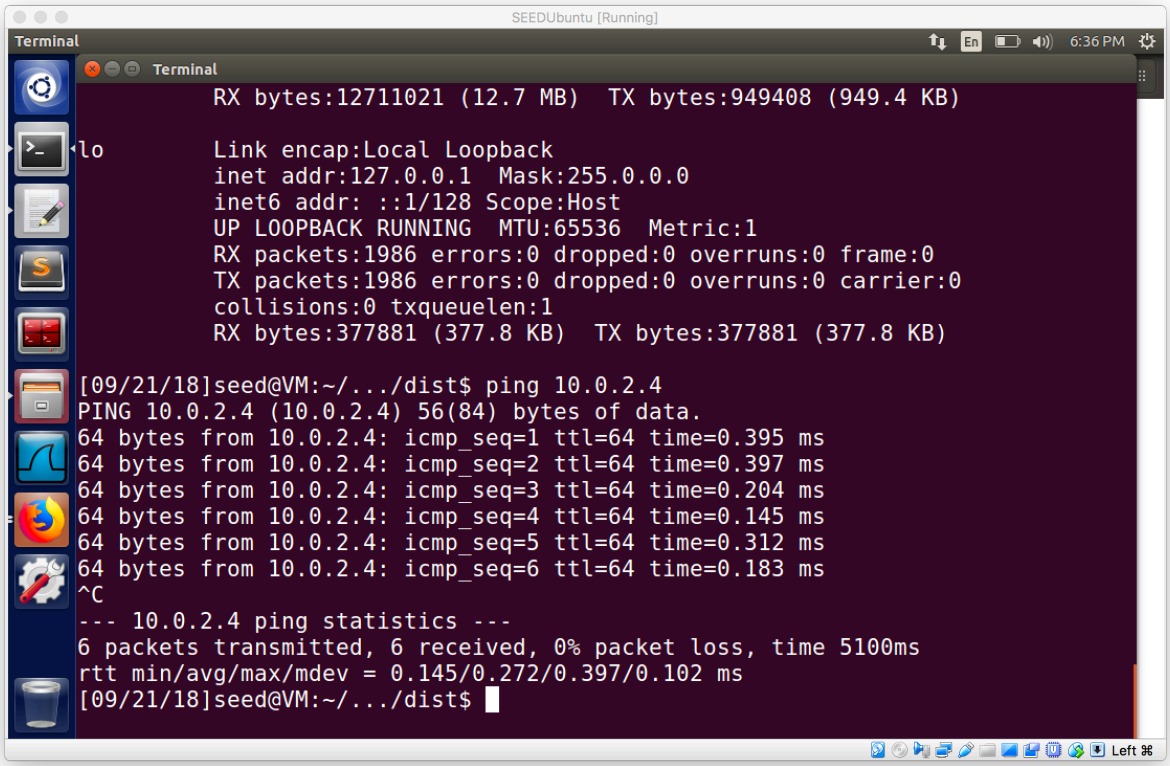


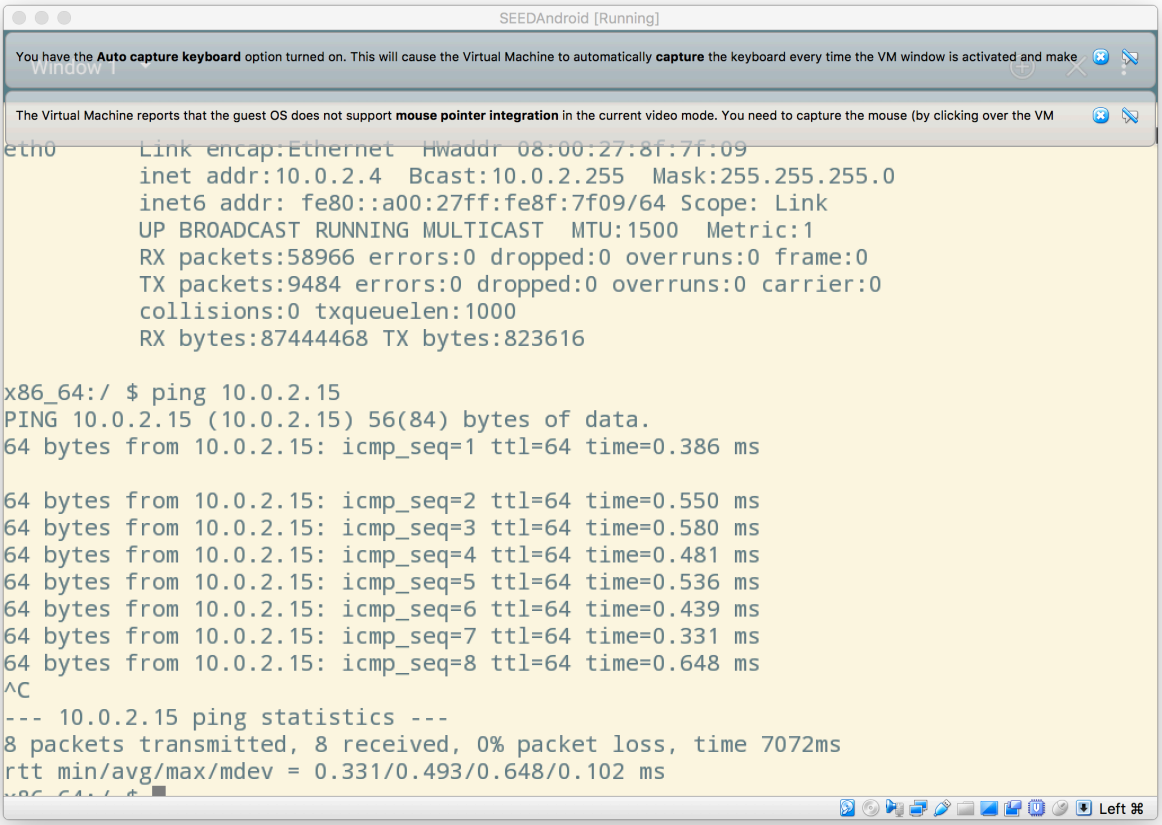
Figure 5

5) Next, we use the ifconfig command to check the IP address of the VM on both the machines (SEED Android & SEEdD Ubuntu) and ping each other to check the connectivity. Below are the attached screenshots.


SEEDUbuntu [Running]
Terminal
6:25 PM
Terminal
The signer certificate will expire within six months.
No -tsa or -tsacert is provided and this jar is not timestamped. Without a ti
mestamp, users may not be able to validate this jar after the signer certific
ate's expiration date (2018-12-20) or after any future revocation date.
[09/21/18]seed@VM:~/.../dist$ ifconfig
enp0s3 Link encap:Ethernet HWaddr 08:00:27:dc:52:38
inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::2425:8ca0:90cf:d8f8/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:13766 errors:0 dropped:0 overruns:0 frame:0
TX packets:7447 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:12711021 (12.7 MB) TX bytes:949408 (949.4 KB)
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:1986 errors:0 dropped:0 overruns:0 frame:0
TX packets:1986 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:377881 (377.8 KB) TX bytes:377881 (377.8 KB)
[09/21/18]seed@VM:~/.../dist$
Left ⌘

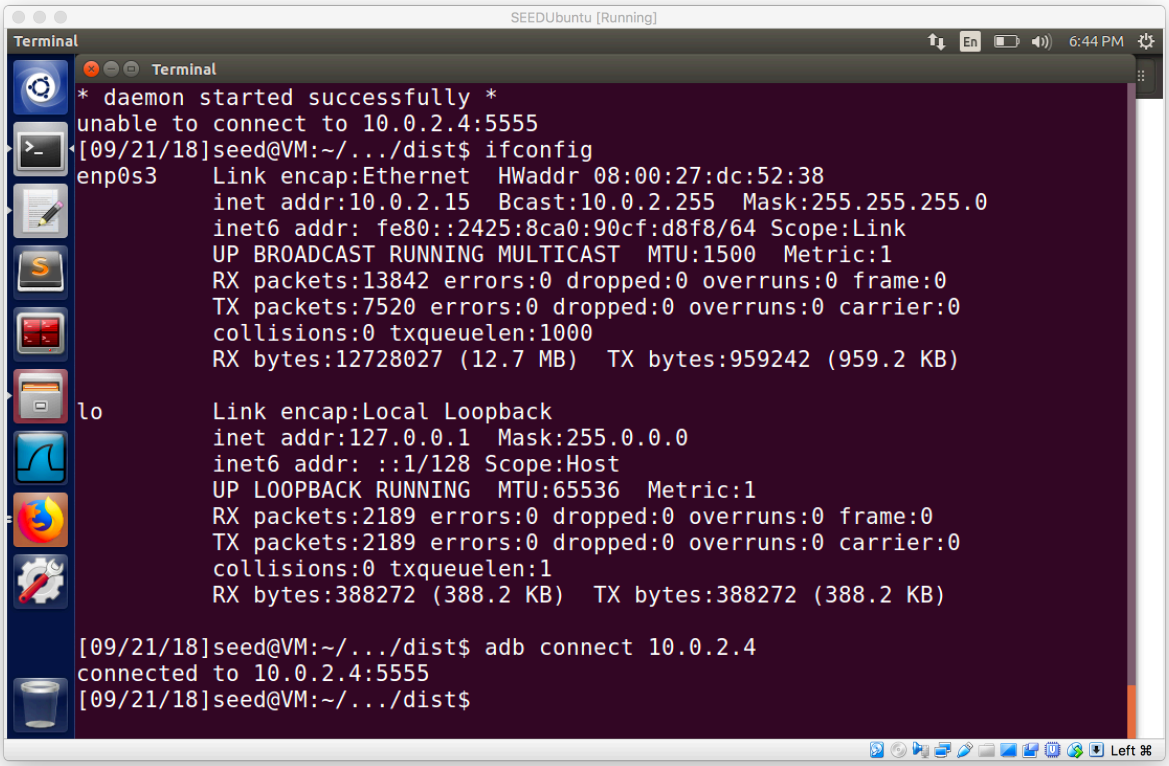

SEEDAndroid [Running]
You have the Auto capture keyboard option turned on. This will cause the Virtual Machine to automatically capture the keyboard every time the VM window is activated and make
The Virtual Machine reports that the guest OS does not support mouse pointer integration in the current video mode. You need to capture the mouse (by clicking over the VM
From 10.0.2.4: icmp_seq=6 Destination Host Unreachable
^C
--- 10.0.2.15 ping statistics ---
8 packets transmitted, 0 received, +6 errors, 100% packet loss, time 7177ms
pipe 3
1|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:15 errors:0 dropped:0 overruns:0 frame:0
TX packets:15 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:1680 TX bytes:1680
eth0 Link encap:Ethernet HWaddr 08:00:27:8f:7f:09
inet addr:10.0.2.4 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe8f:7f09/64 Scope: Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:58951 errors:0 dropped:0 overruns:0 frame:0
TX packets:9438 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:87441049 TX bytes:819764
Left ⌘


SEEDUbuntu [Running]
Terminal
6:36 PM
Terminal
RX bytes:12711021 (12.7 MB) TX bytes:949408 (949.4 KB)
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:1986 errors:0 dropped:0 overruns:0 frame:0
TX packets:1986 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:377881 (377.8 KB) TX bytes:377881 (377.8 KB)
[09/21/18]seed@VM:~/.../dist$ ping 10.0.2.4
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.395 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.397 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.204 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.145 ms
64 bytes from 10.0.2.4: icmp_seq=5 ttl=64 time=0.312 ms
64 bytes from 10.0.2.4: icmp_seq=6 ttl=64 time=0.183 ms
^C
--- 10.0.2.4 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5100ms
rtt min/avg/max/mdev = 0.145/0.272/0.397/0.102 ms
[09/21/18]seed@VM:~/.../dist$
Left ⌘

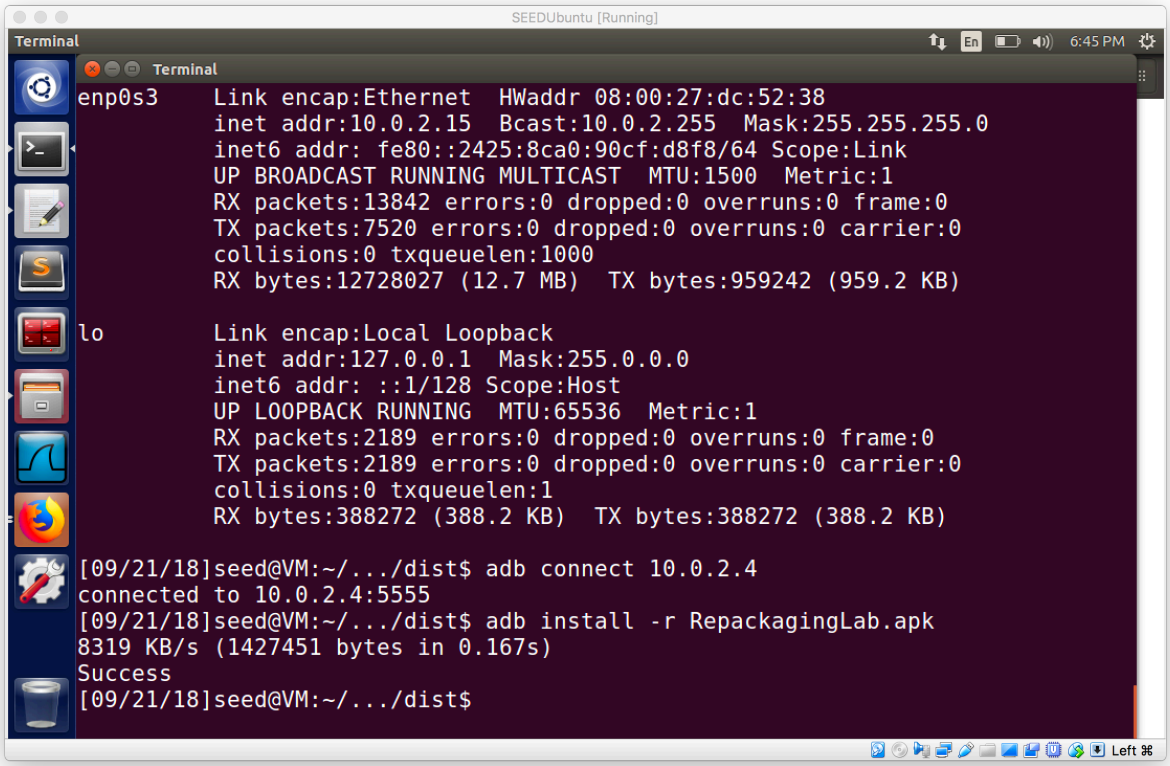


As we see, the machines are able to ping each other perfectly and there is 0% packet loss.

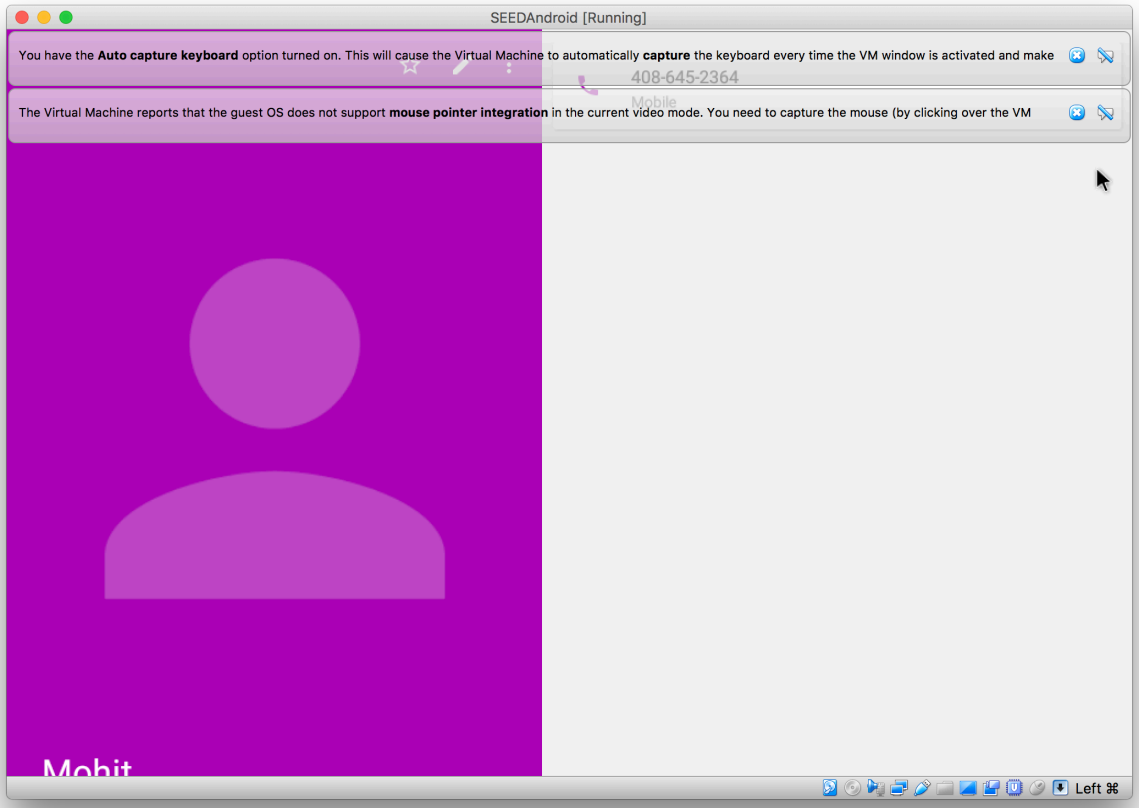
6) We use **adb** to establish a secure connection from the SEED Ubuntu to the Android VM.



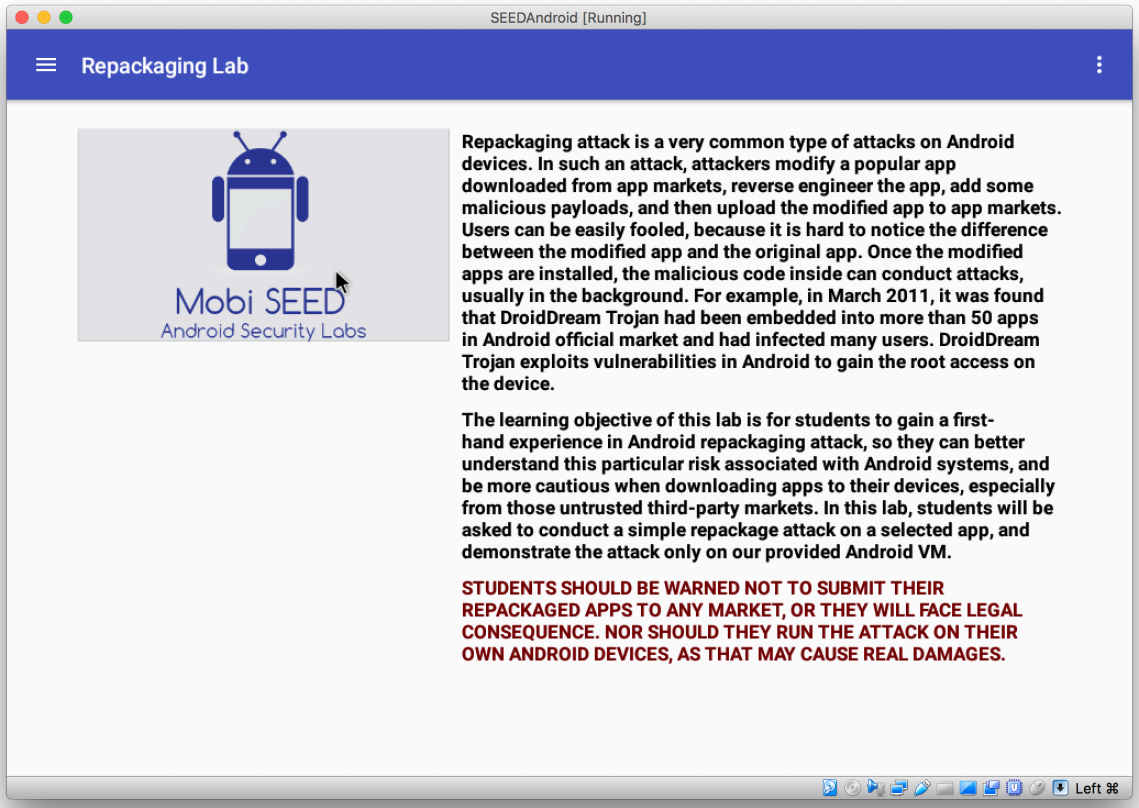
7) Next, we install the repackaged app into our Android VM through the adb connection we had establishes earlier. Below is the screenshot.



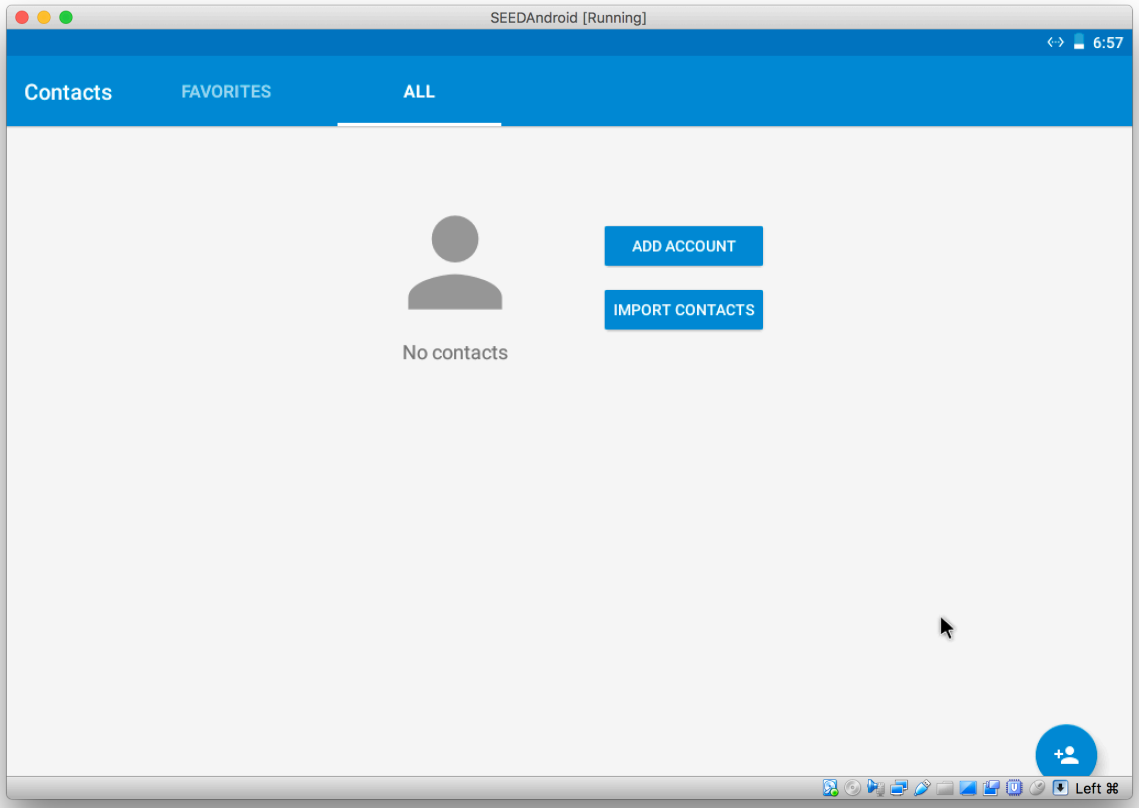
8) Next, we create a contact on the Android VM.



9) Now, we launch our installed app.



10) After rebooting our VM, we come to know that all our contacts have been deleted.


SEEDAndroid [Running]
6:57
Contacts
FAVORITES
ALL
ADD ACCOUNT
IMPORT CONTACTS
No contacts
Left ⌘