**REPACKAGING LAB**

Contents

[TASK 1 3](#_Toc118404506)

[TASK 2 3](#_Toc118404507)

[TASK 3 4](#_Toc118404508)

[TASK 4 6](#_Toc118404509)

[Task 4.1 6](#_Toc118404510)

[Task 4.2 6](#_Toc118404511)

[TASK 5 8](#_Toc118404512)

[Task 5.1 8](#_Toc118404513)

[Task 5.2 8](#_Toc118404514)

[Task 5.3 9](#_Toc118404515)

[TASK 6 12](#_Toc118404516)

[Task 6.1 12](#_Toc118404517)

[Task 6.2 13](#_Toc118404518)

[Task 6.3 16](#_Toc118404519)

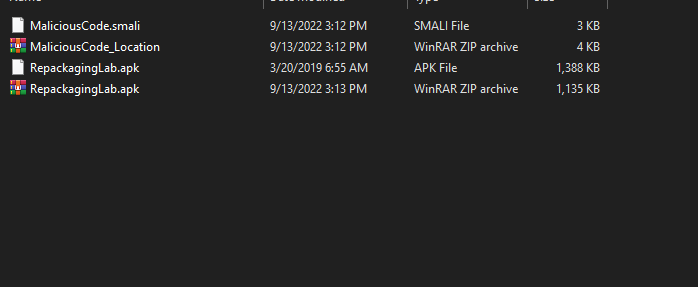
[Task 6.4 17](#_Toc118404520)

[Task 6.5 17](#_Toc118404521)

[Task 6.6 18](#_Toc118404522)

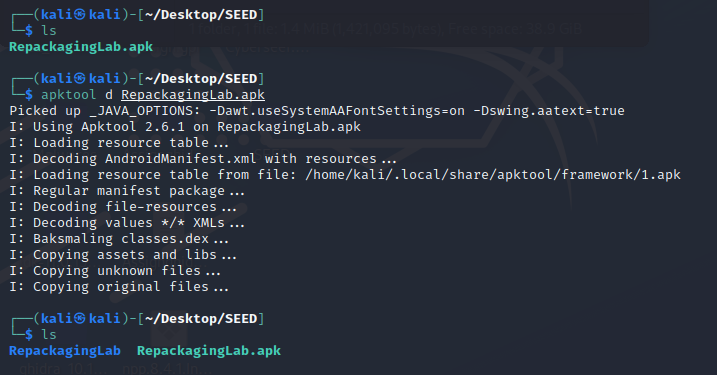
# TASK 1

RepackagingLab an apk of an app provided by SEED Labs is used for for this task

****

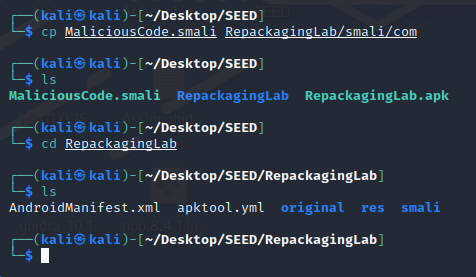
# TASK 2

Decompiling RepackagingLab.pk in Kali Linux with apktool

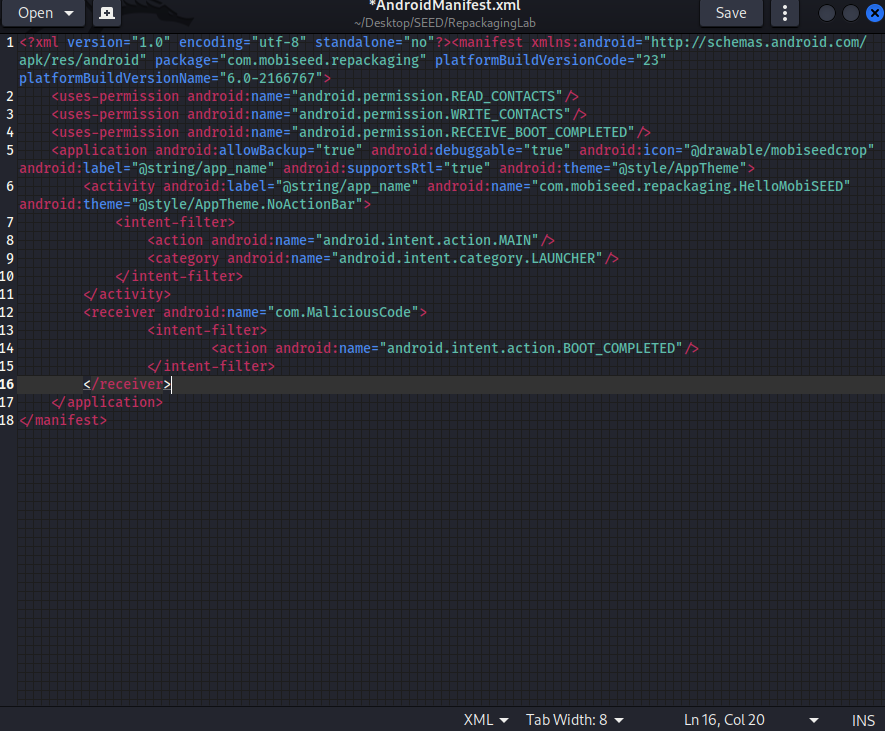
****

# TASK 3

Copying the Malicious Code in Application Specific Folder known as com

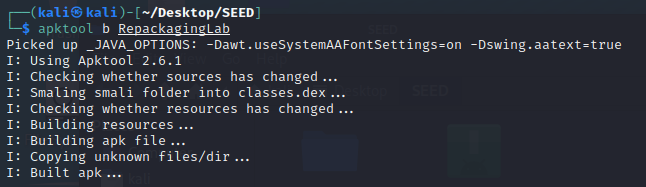


Wrote the code on line 2 to 4 to read and write contacts that’s how we can remove contacts. On line 4 we get permission for boot complete details whereas on line 14 we get boot completed broadcast message. On line 12 the Malicious File to be fetched and used is provided.

****

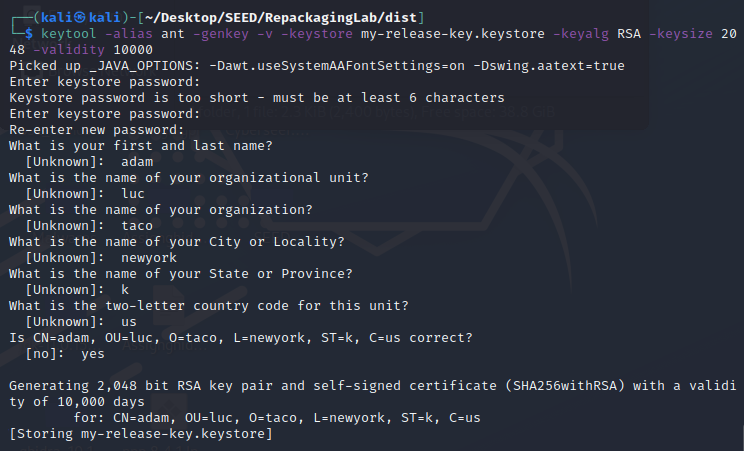
# TASK 4

## Task 4.1

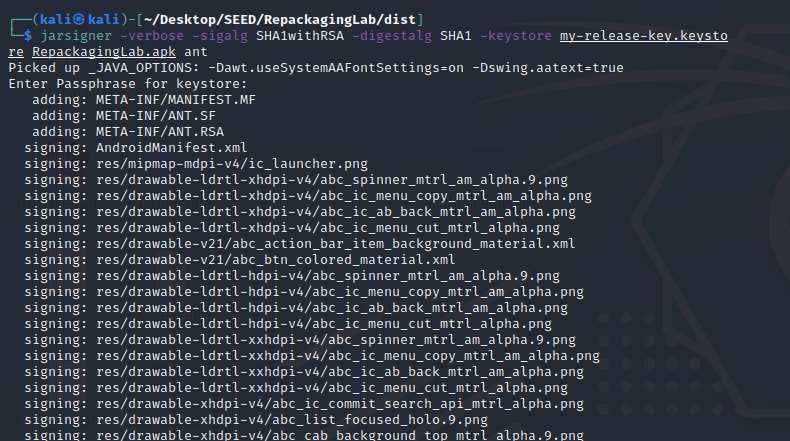
Rebuilding the apk to proceed with signing.****

## Task 4.2

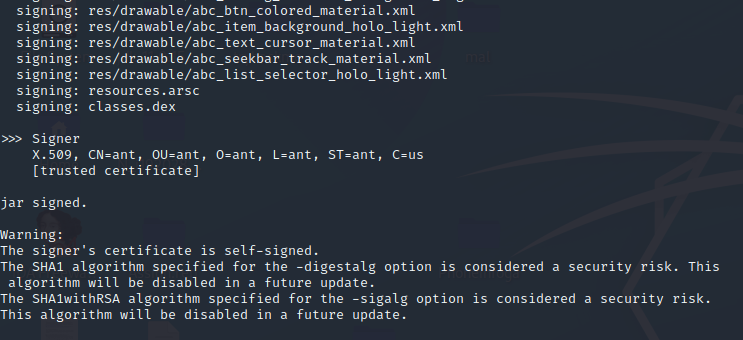
Making a Private Key for signing the apk



Signing apk with jarsigner



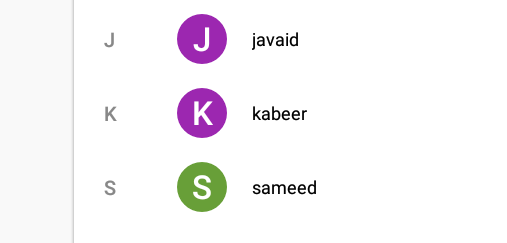
Successfully signed with jarsigner



# TASK 5

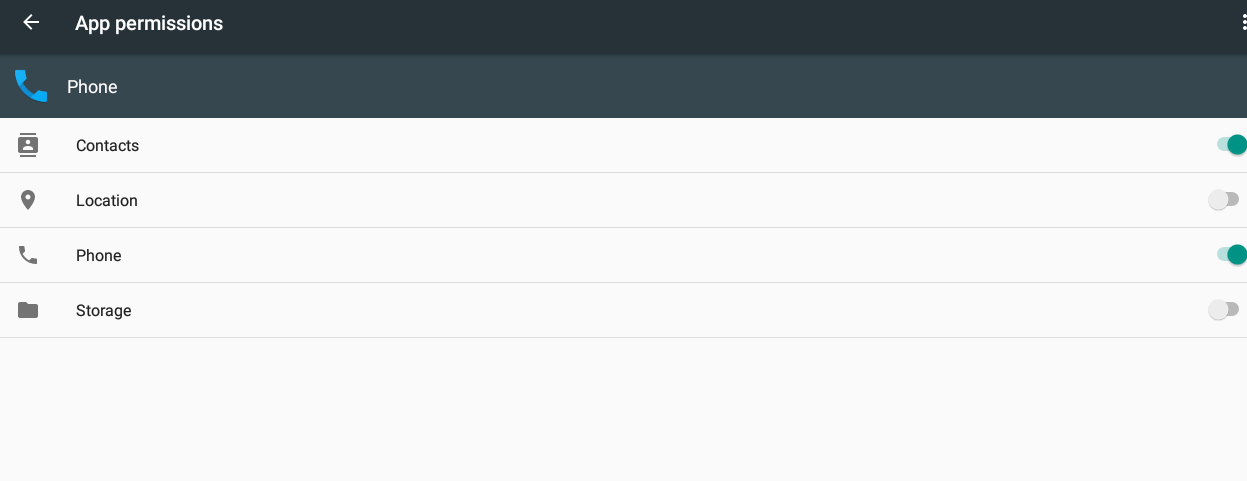
## Task 5.1

Adding Some Contacts for Demonstration of Attack in Android VM

****

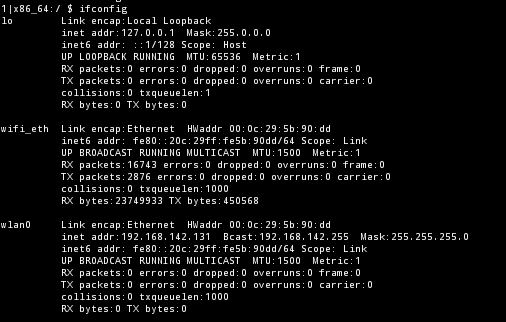
## Task 5.2

Gave Permissions to Contact App

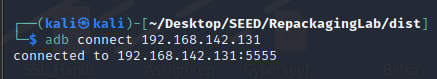
****

## Task 5.3

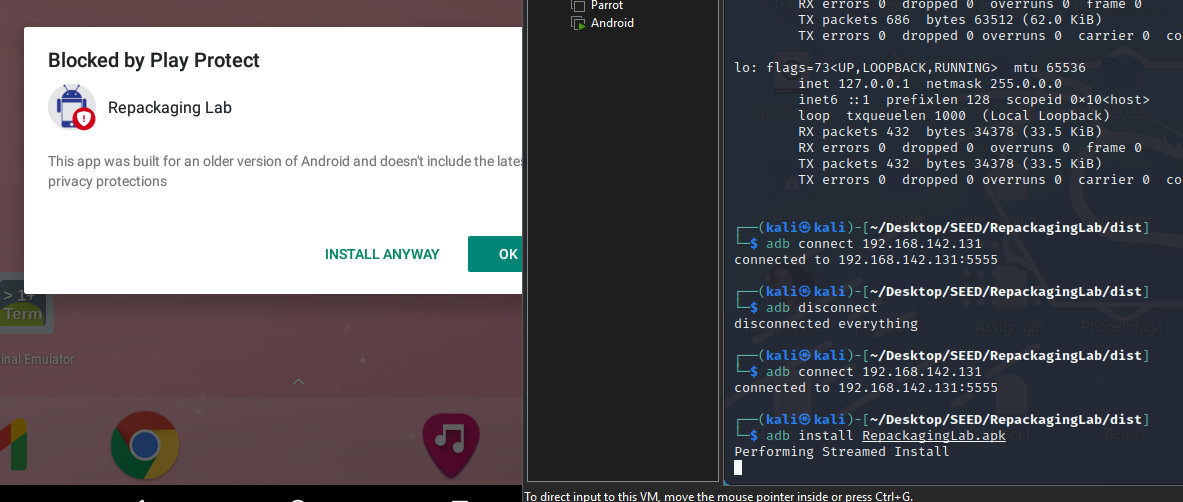
IP of Android VM fetched from it’s terminal

****

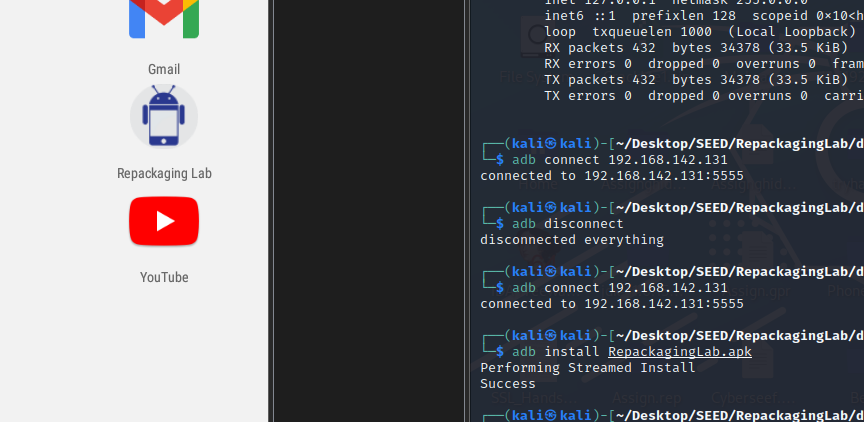
Connecting to Android VM from Attacker VM

****

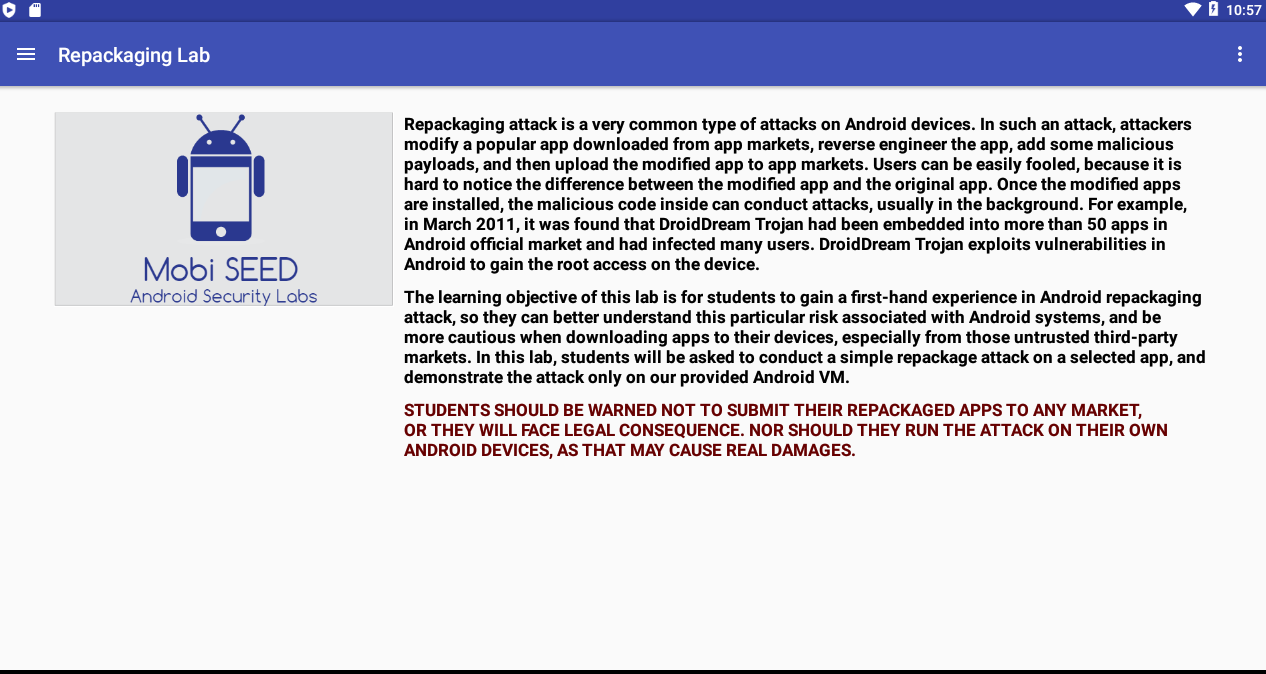
Injecting Playload and Installing it on Android VM

****

Malicious Payload Successfully Injected

****

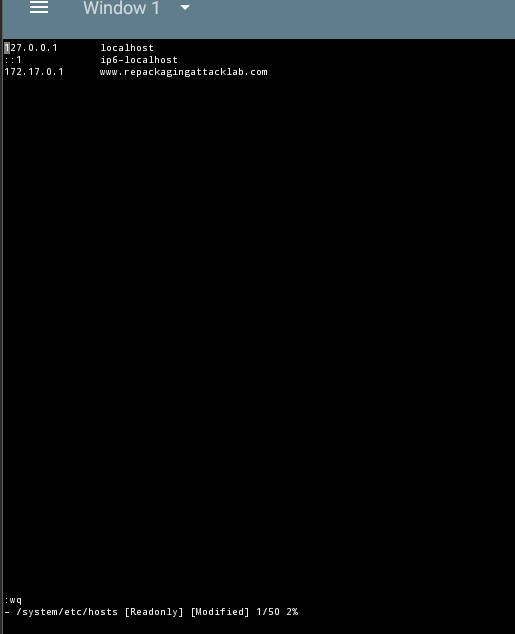
View of Repackaging Apk after installation

****

# TASK 6

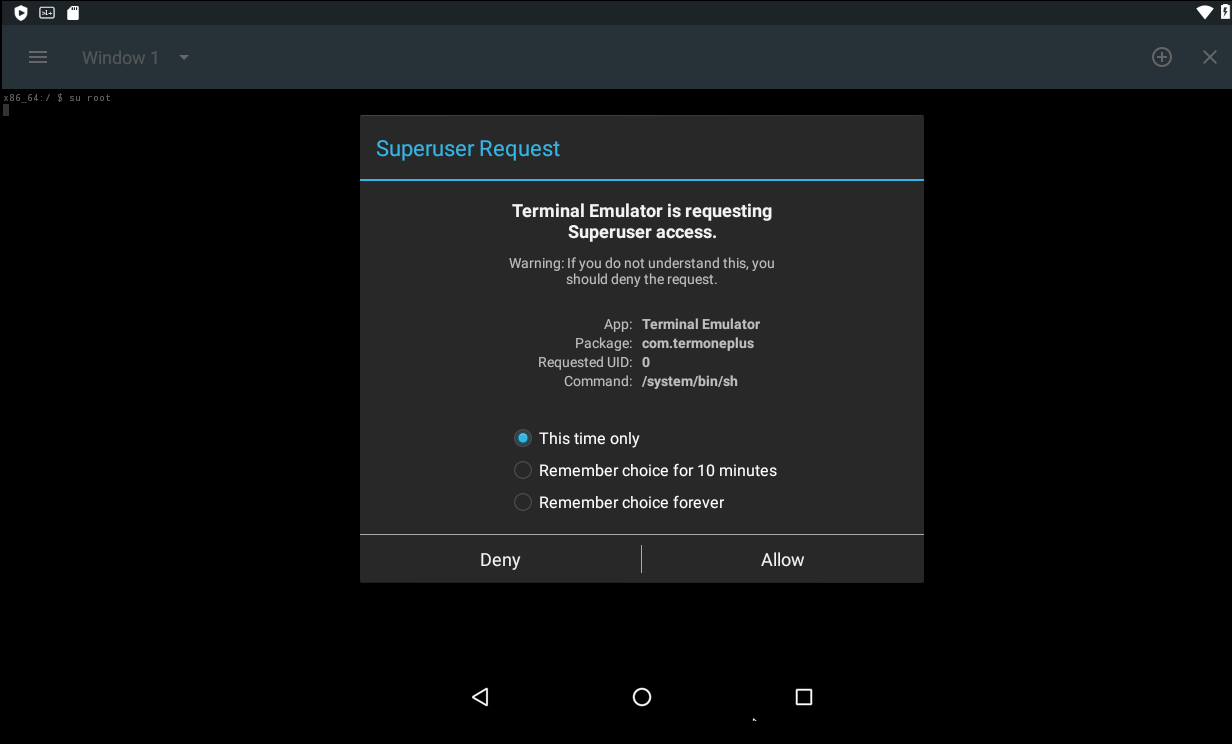
## Task 6.1

To track the victim first providing victim machine with Attacker VM IP as host

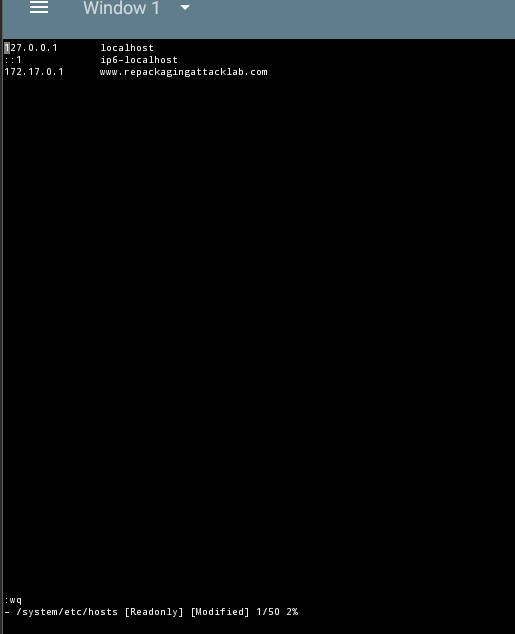
****

## Task 6.2

Allowing Root Access to the Terminal

****

To track the victim first providing victim machine with Attacker VM IP as host

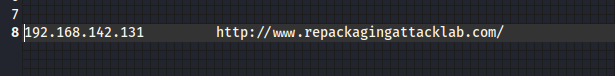
****

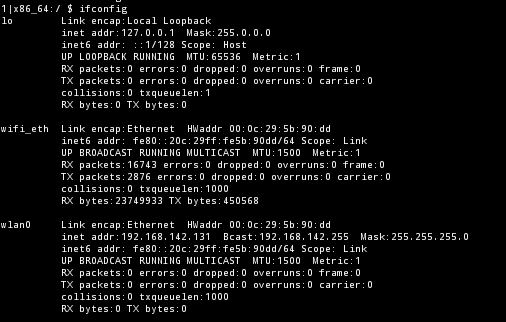
Pulling Hosts file from Android VM

****

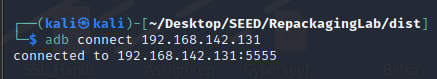
Adding Victim IP in Attacker VM

****

****

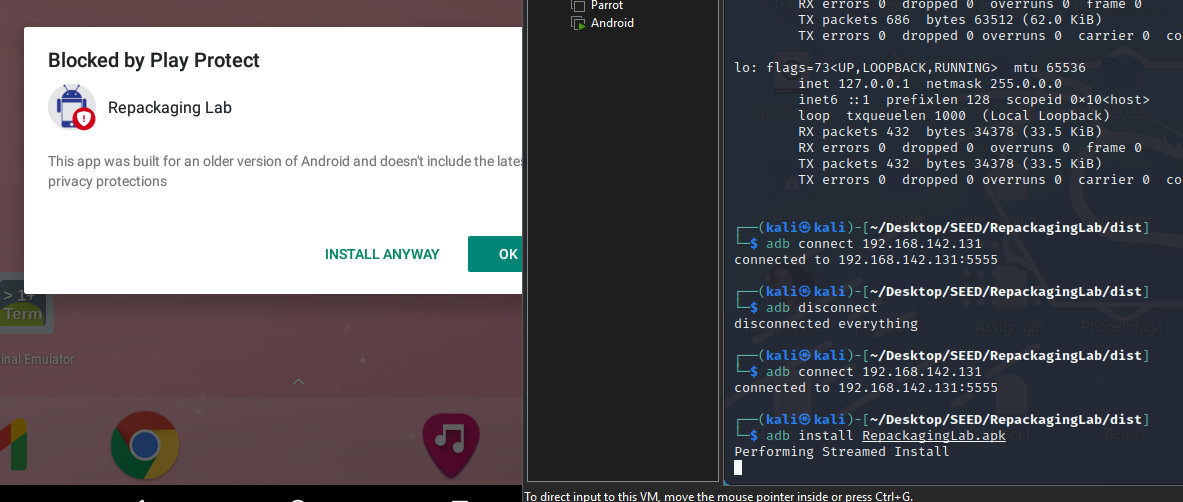
****

Connecting with Victim Machine

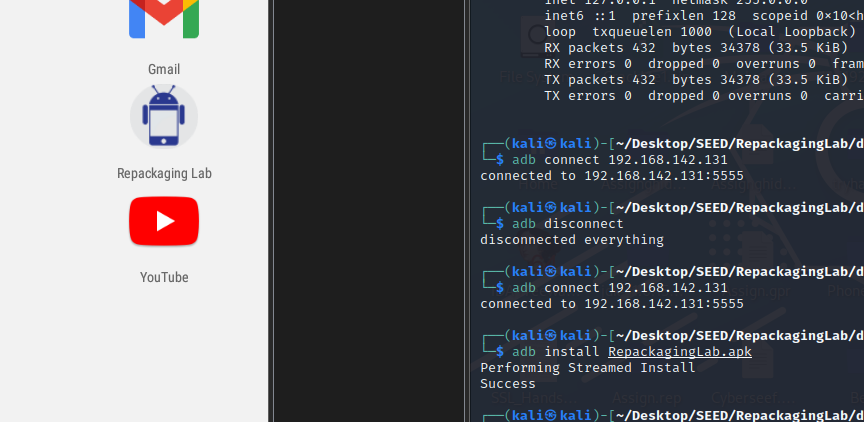
****

## Task 6.3

Injecting Playload and Installing it on Android VM

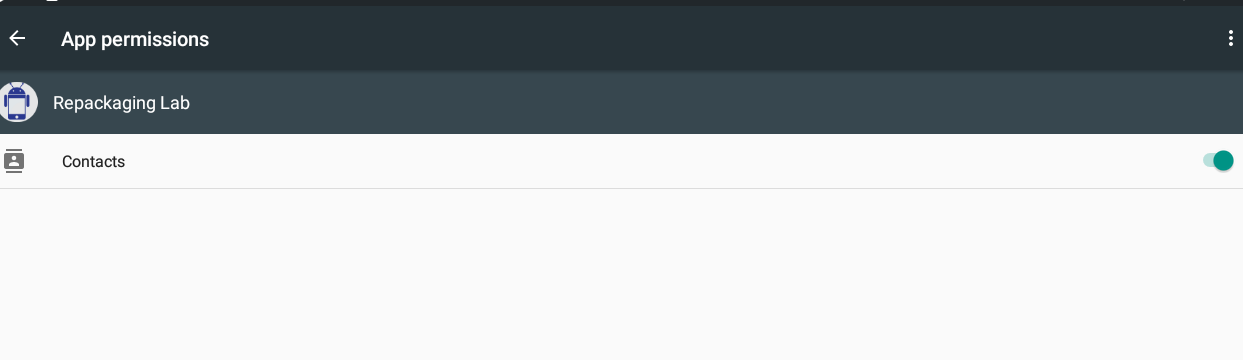
****

Malicious Payload Successfully Injected

****

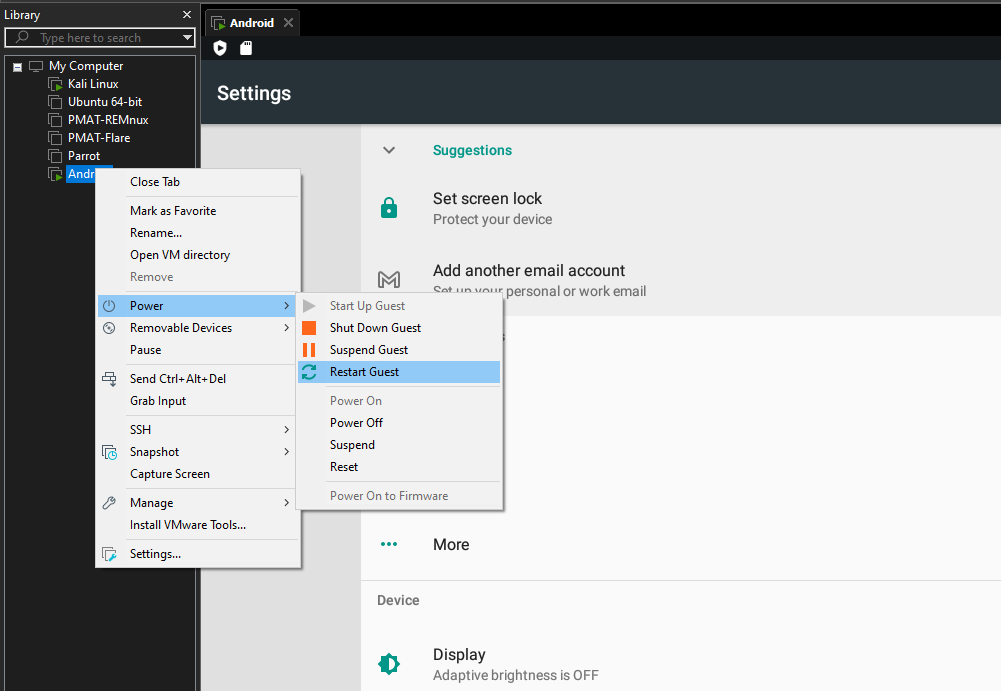
## Task 6.4

Giving Permissions to Repackaging Lab apk to access contacts on Android VM

****

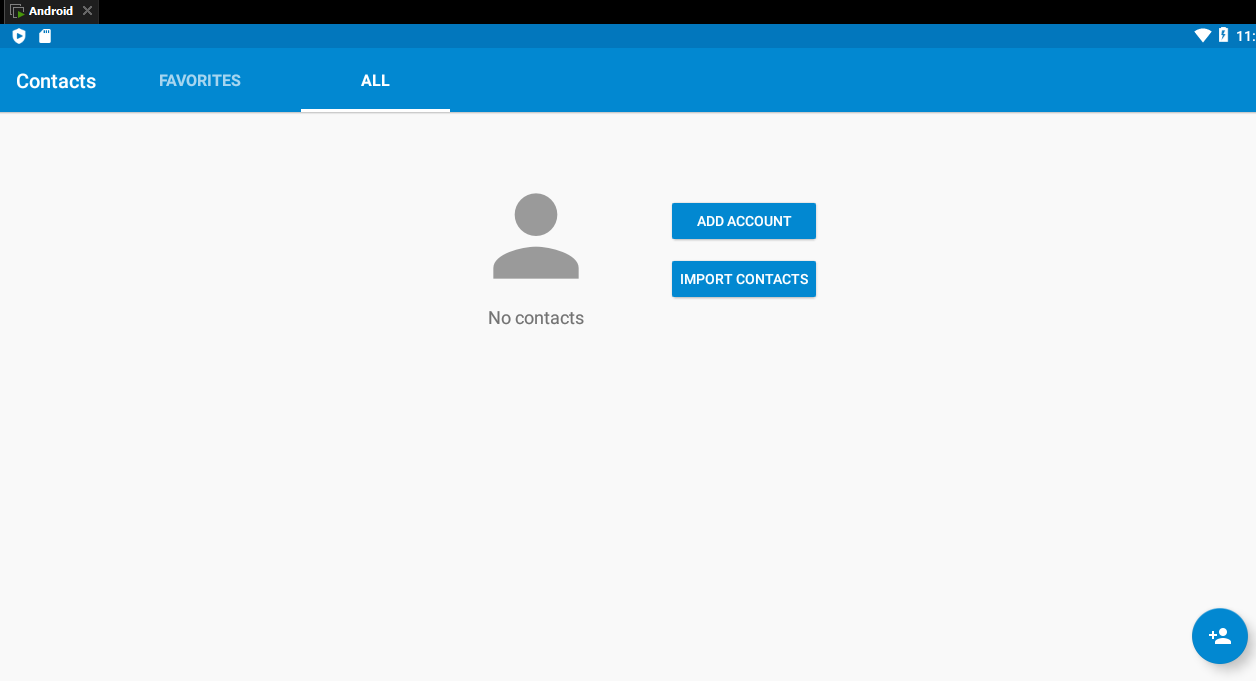
## Task 6.5

Restarting Android VM to initiate Repackaging Attack

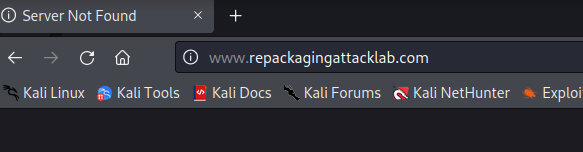
****

## Task 6.6

End Result Victim Lost Contacts



Attack can be Tracked via this link on Attacker VM but due to internet issues the working screenshot couldn’t be taken

****