Android Penetration Testing

Lab Setup: -

1. Virtual BOX

* <https://www.virtualbox.org/>

1. Santoku OS

* <https://santoku-linux.com/>

1. Geny Motion

* <https://genymotion.com/>
* Virtual Box
* https://www.virtualbox.org/
* First Download VirtualBox
* Normally install like other application we install

Santoku OS Installation

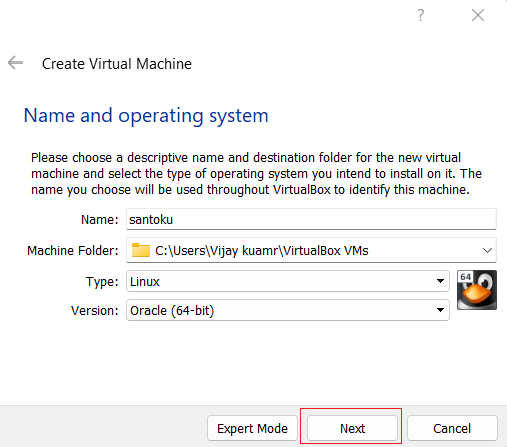
1. First Download Santoku OS

<https://santoku-linux.com/>

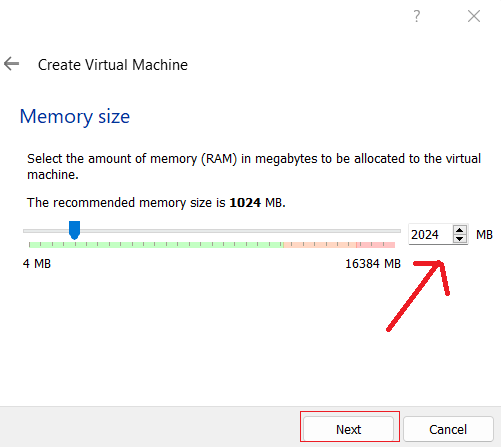
1. Then Open virtual box which we installed –
   * + - Then click new-

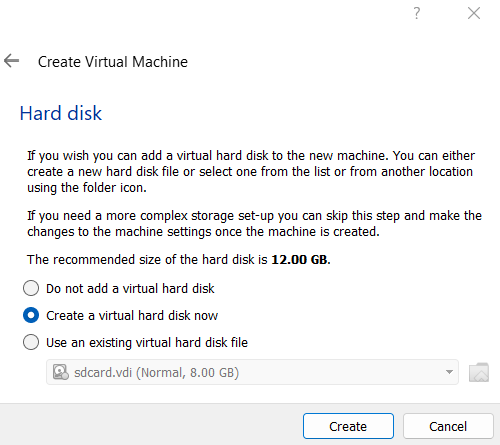


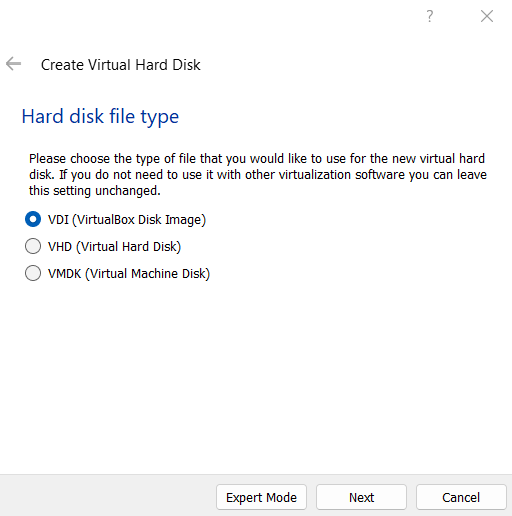
* + - * Then type name and choose machine folder where do you want install, select OS type and OS version and then click next.

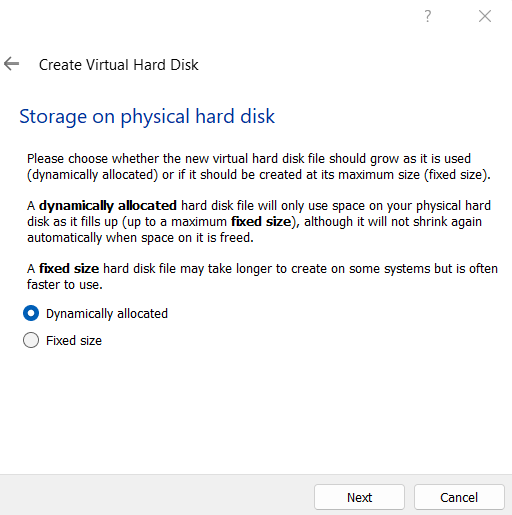


* + - * Then select memory size –

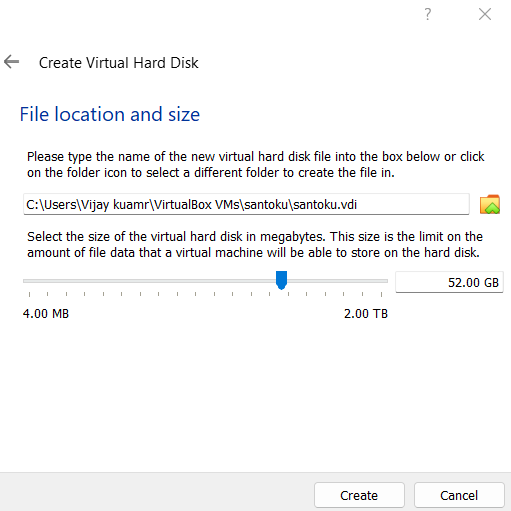


* + - * Then click Create,-
      * and click next next if you want change then you can-





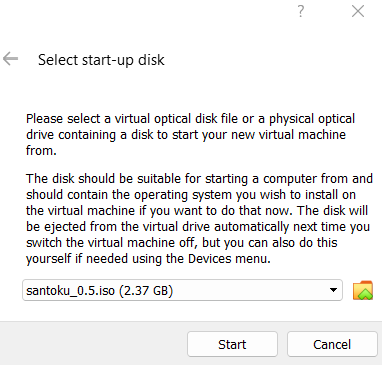
* + - * Then select File location and click create button -



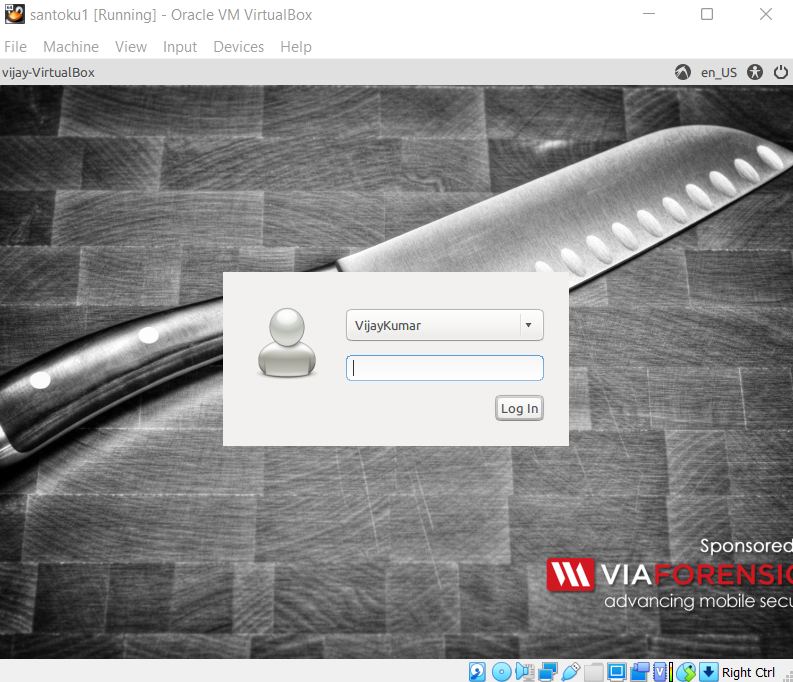
1. After Create Santoku OS then click Start –



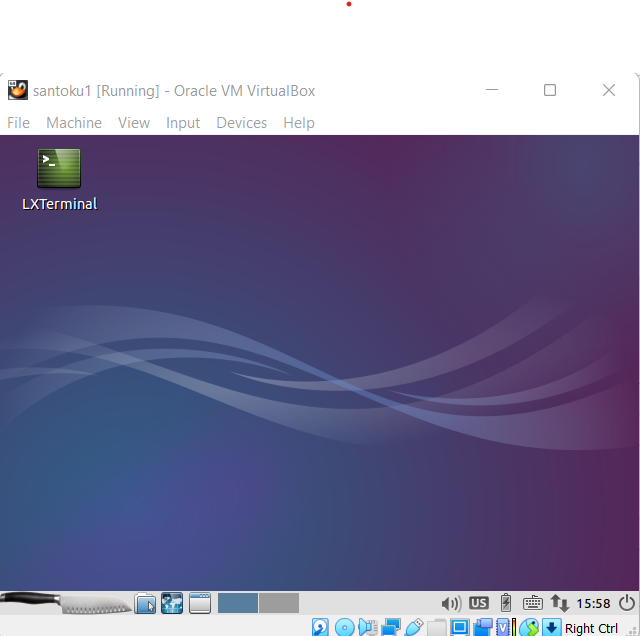
1. Then Select Santoku iso which you downloaded and click start-



* Its take some time and ask something like language, user name, password etc.
* Finally your santoku OS look like- enter you password and login



* After login Santoku OS look like-



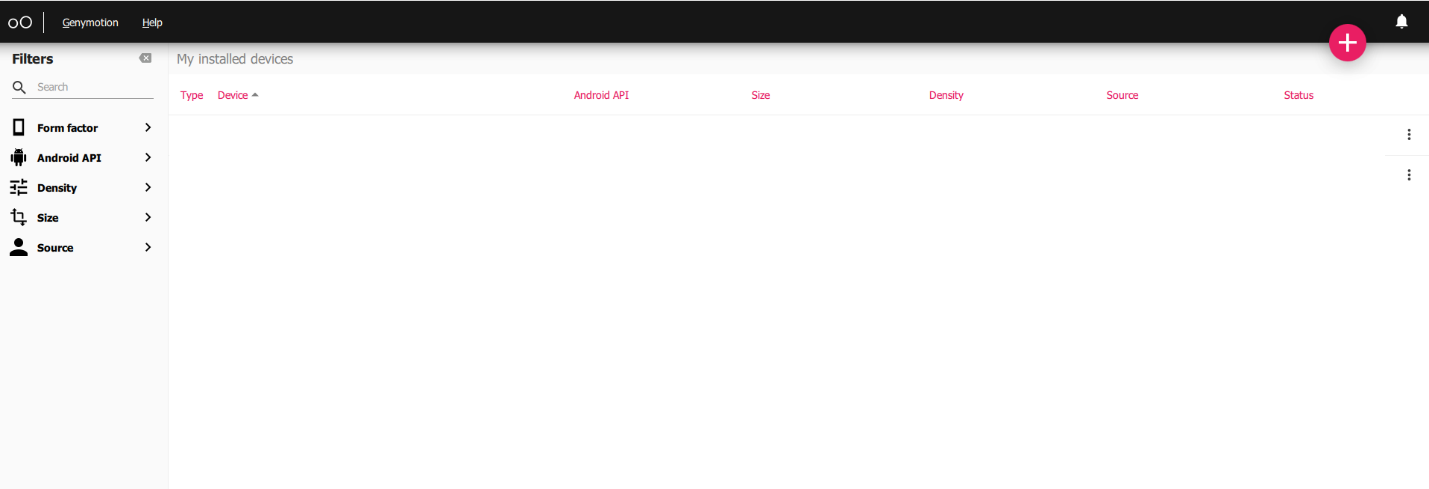
Now Your Santoku OS ready to doing work.

GenY Motion installation

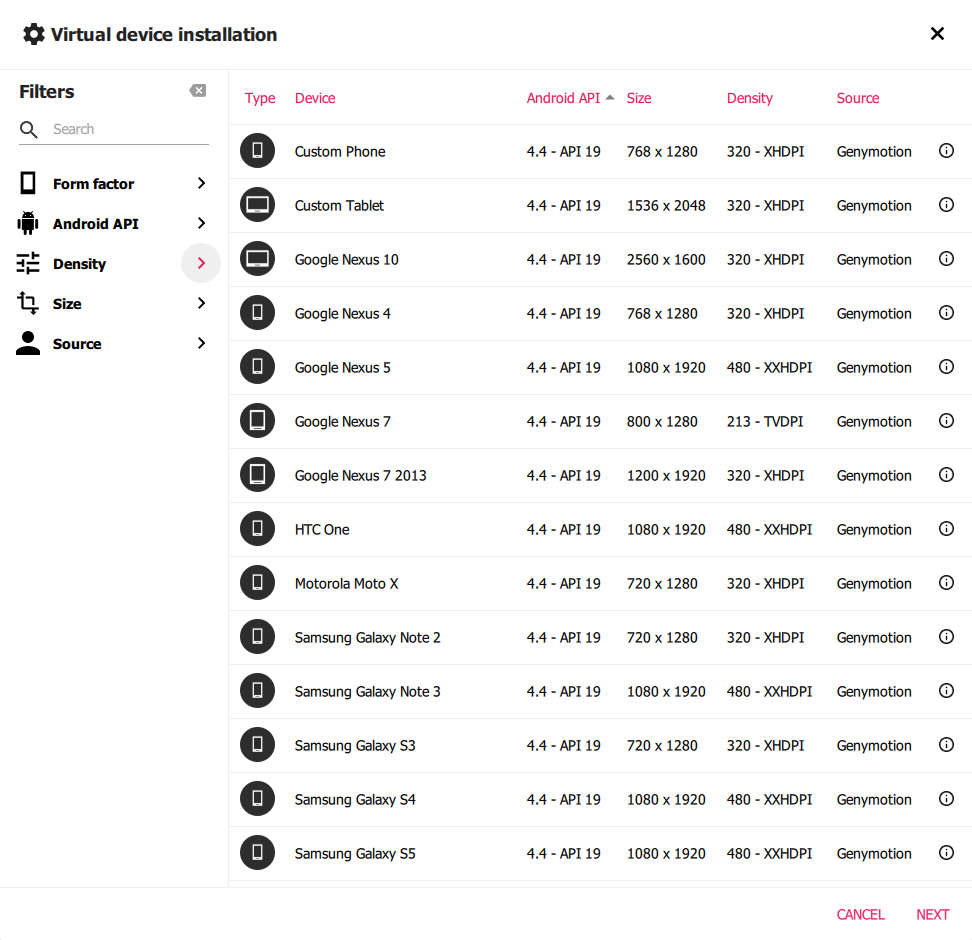
1. Download GenY motion

* <https://genymotion.com/>

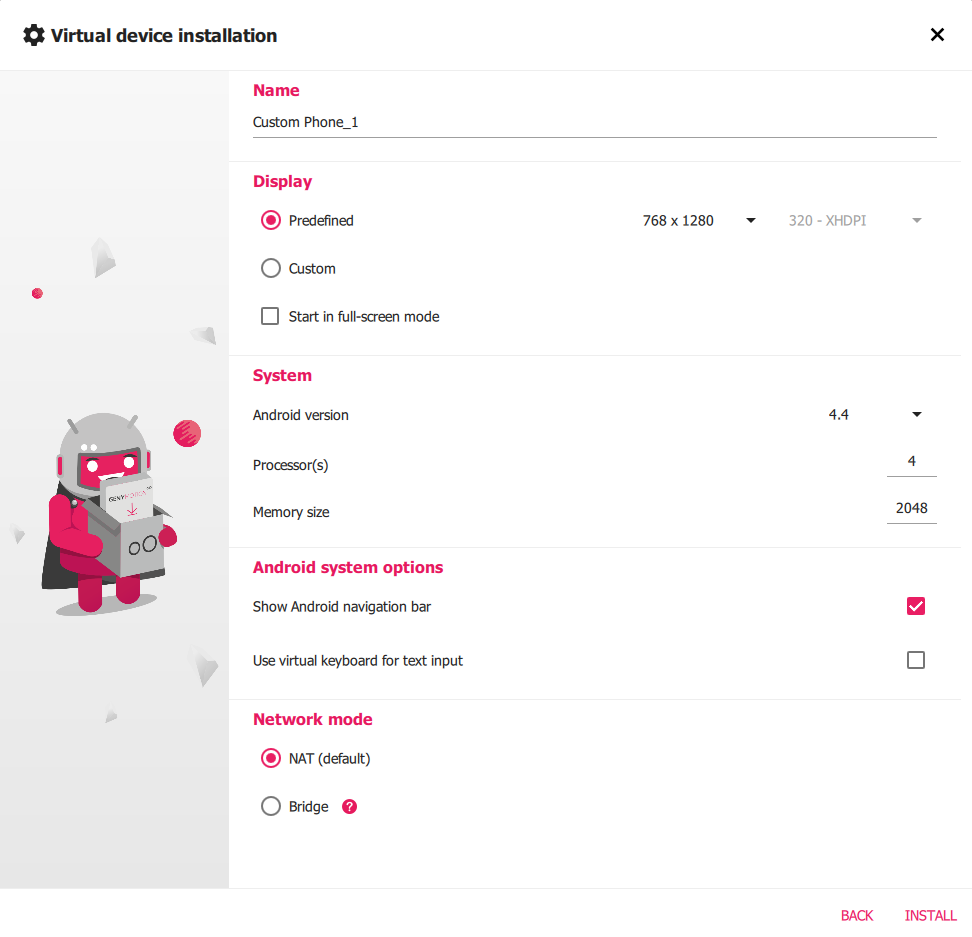
1. After download normally install like other application we installed.
2. After installing you create GenY motion account and login .
3. After login you GenY Motion look like-



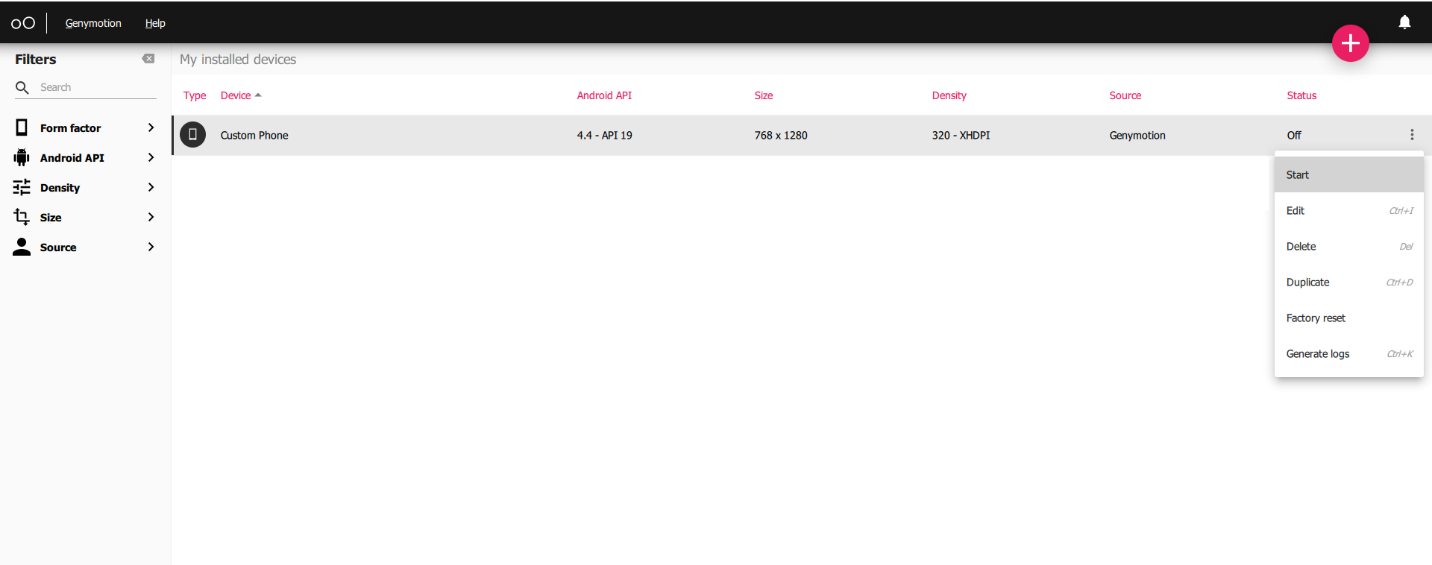
1. Then click on add button and select any device which version you want to install.



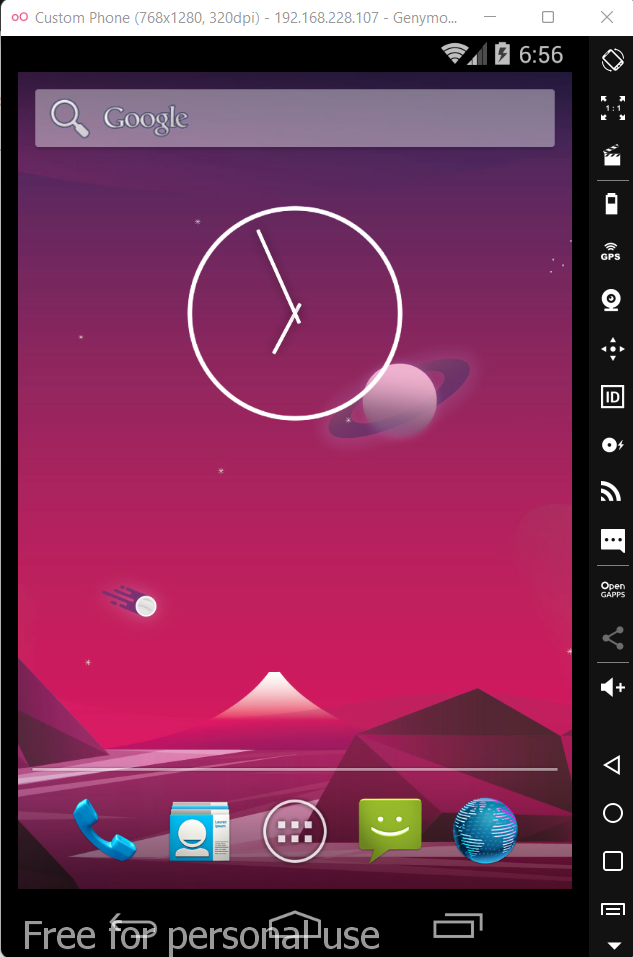
1. And configure device as your requirement and install



1. After installing click on start button-



1. After start your devices look like-



Now our lab setup complete.

Let’s Start Practical: -

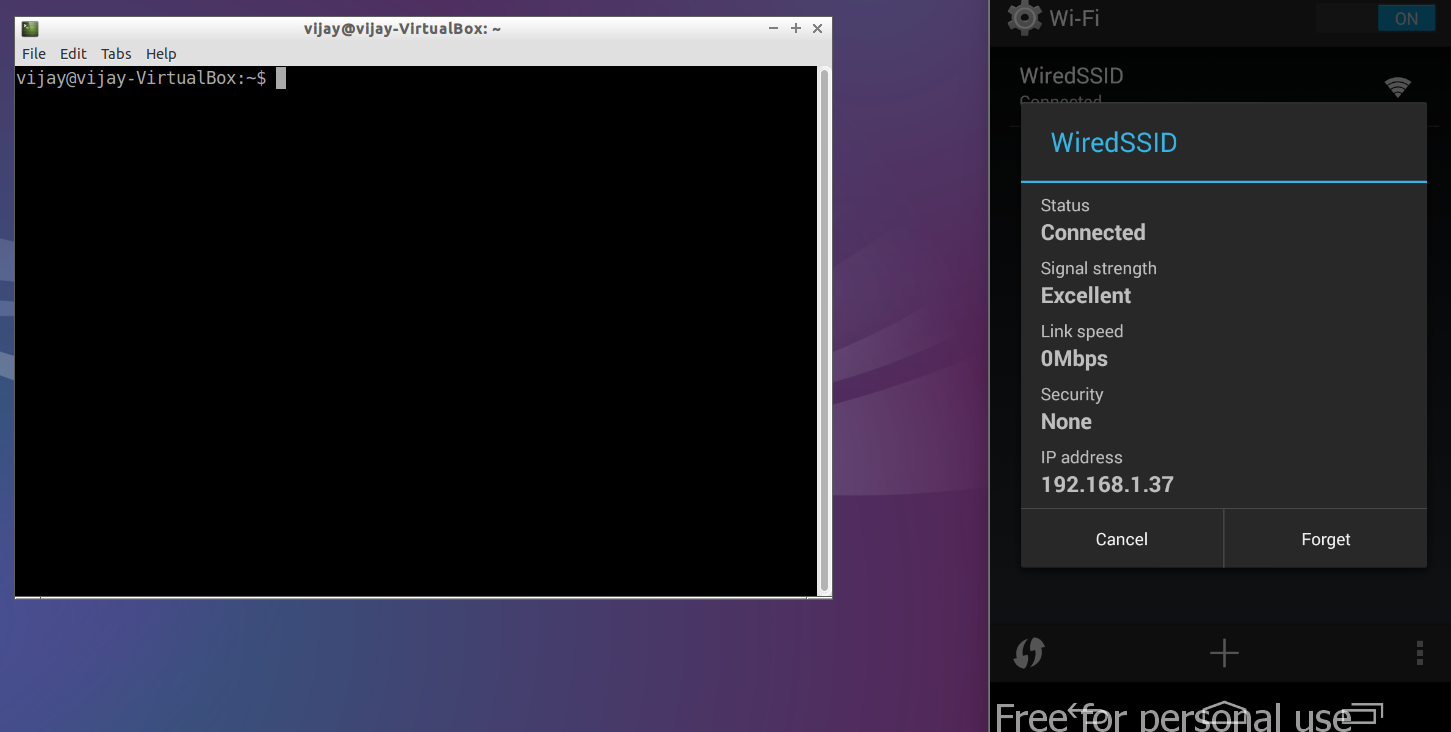
* + - * Adb Practical: -

1. adb connect <ip>(for connecting with phone)
2. adb devices (for checking connected devices)
3. adb disconnect (for disconnecting with phone)
4. adb shell (for get remote terminal of target devices)
5. adb install <application name>(for installing any application in target devices.)
6. adb uninstall <application name>(for installing any application in target devices.)
7. adb logcat (for get logs targeted devices)

For example –

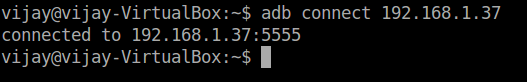
adb connect, adb devices, adb disconnect: -

* First, we open our santoku OS and GenY motion added device
* Then open santoku terminal.
* And also check check genymotion phone ip which we added.
* Look like-



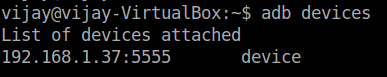
Now –

$ adb connect 192.168.1.37 //target device ip address and enter



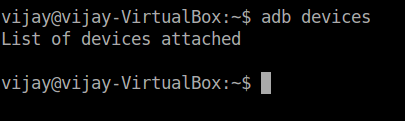
* + - * Its connected.

$adb devices //for checking connect devices



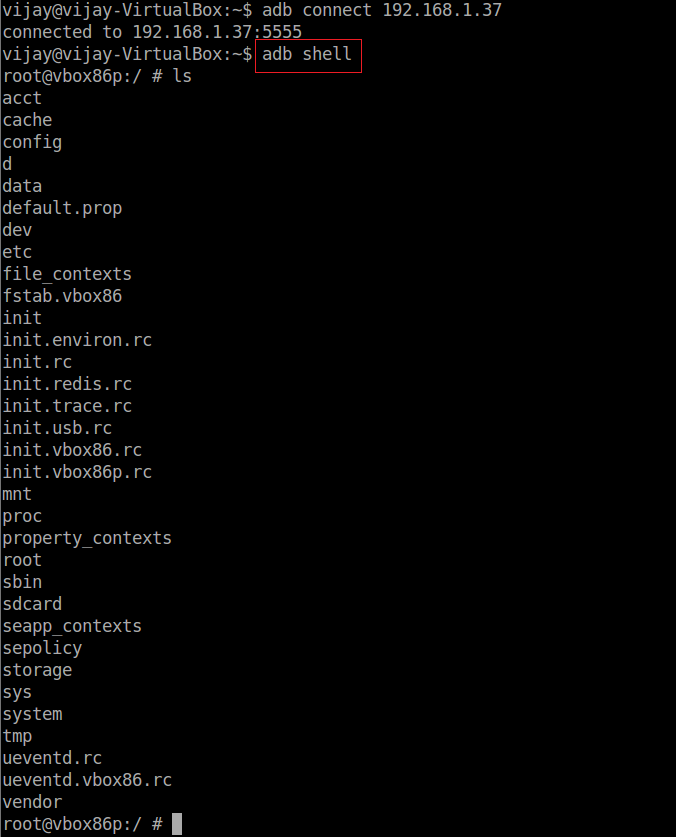
* Here one connected device found

$adb disconnect //for disconnecting devices



* After disconnect command no devices connected

$adb shell // for get remote terminal of target devices



* adb shell give all file or data available on our target devices.

adb install and adb uninstall any application in target devices we will see later.

Android Application Penetration Testing

Requirement: -

1. Any vulnerable application(In this I use DIVA app)
2. Apk tool
3. Jadx
4. unzip

Steps: -

1. Download vulnerable application (DIVA)

<https://github.com/0xArab/diva-apk-file.git/>

1. Download jadx

<https://github.com/skylot/jadx/releases/tag/v0.6.0/>

1. install apktool

$ sudo apt-get install apktool (in Santoku OS)

1. install unzip

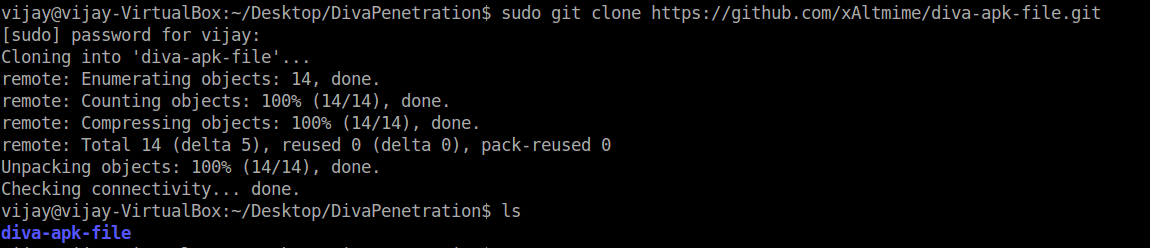
$ sudo apt-get install unzip (in Santoku OS)

Diva: -

* First download diva

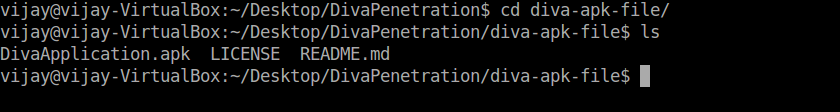
<https://github.com/payatu/diva-android.git/>

$ sudo git clone https://github.com/payatu/diva-android.git/



* Diva downloads successfully
* Now go to diva-apk-file

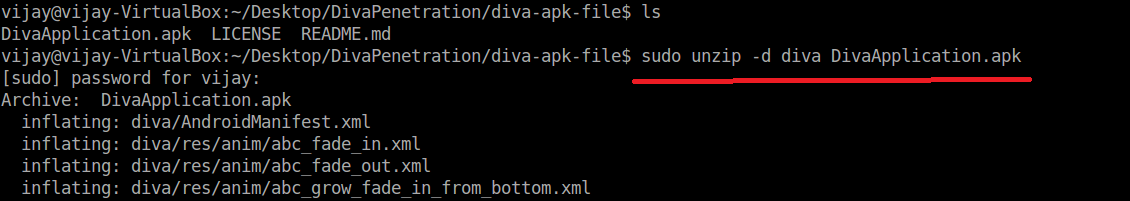
$ cd diva-apk-file



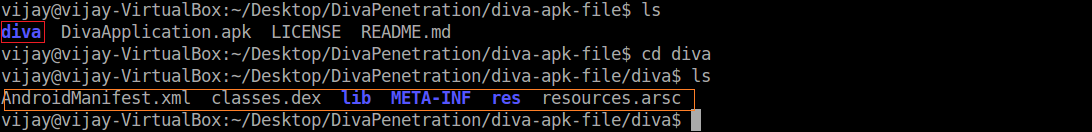
* Then Unzip DivaApplication.apk (without unzip we can’t see any file )

It mens first unzip apk then see all apk file

$ unzip -d diva DivaApplication.apk



* After unzip we find like this type



Now we have all diva file.

Jadx: -

1. First download jadx and unzip same like diva.apk

<https://github.com/skylot/jadx/releases/tag/v0.6.0/>

1. After unzip, jadx look like

