Worcester Polytechnic Institute
Department of Computer Science

Lab 5-Module 9.1: Bypassing Android Lock Screen

Objectives

- Create a virtual Android phone in Santoku Linux.
- Learn the technique to bypass Android lock screen.

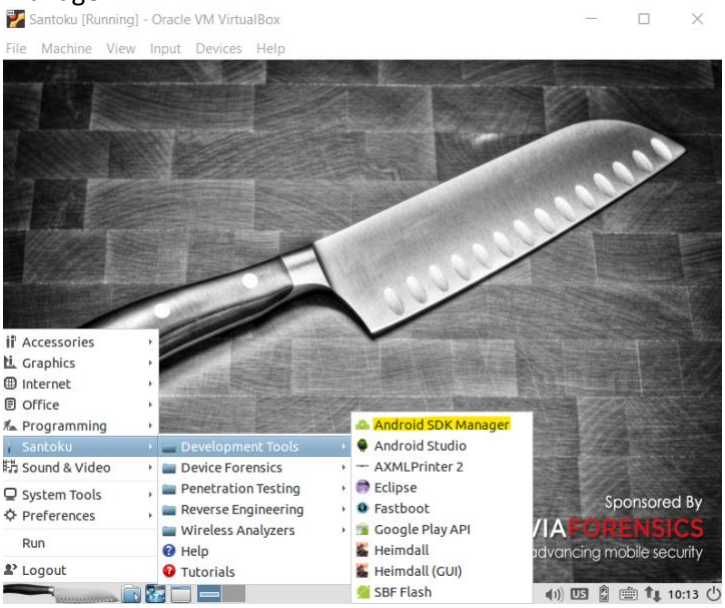
Task

Task 1. Software Preparation

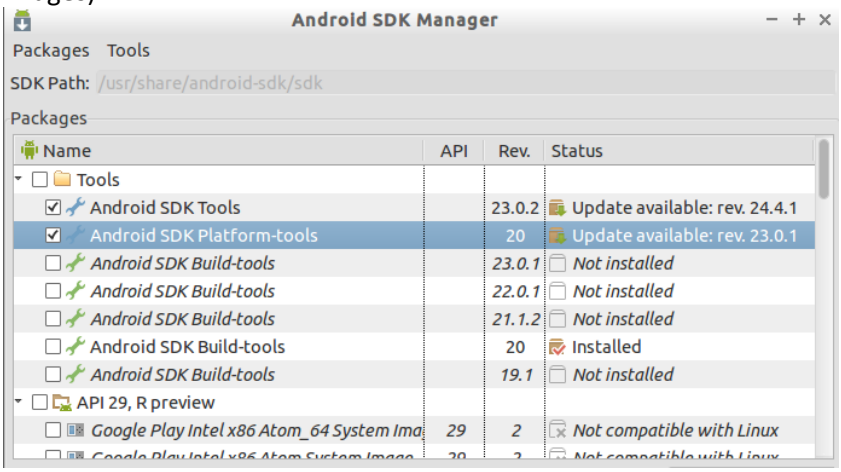
1. Download Santoku from the provided link (from Canvas).
The username and the password of are both santoku.

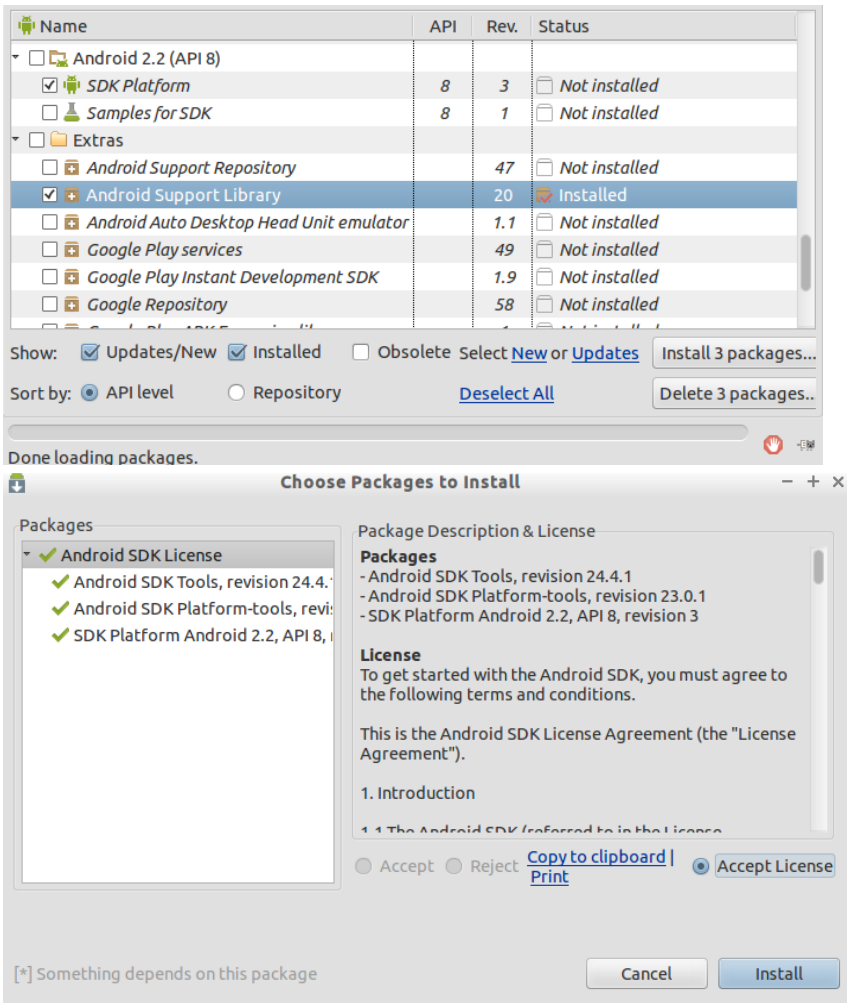
Task 2. Create a virtual Android device.

2. Click the 'knife' icon on the left corner, choose 'Santoku' -> 'Development Tools' -> 'Android SDK Manager'.

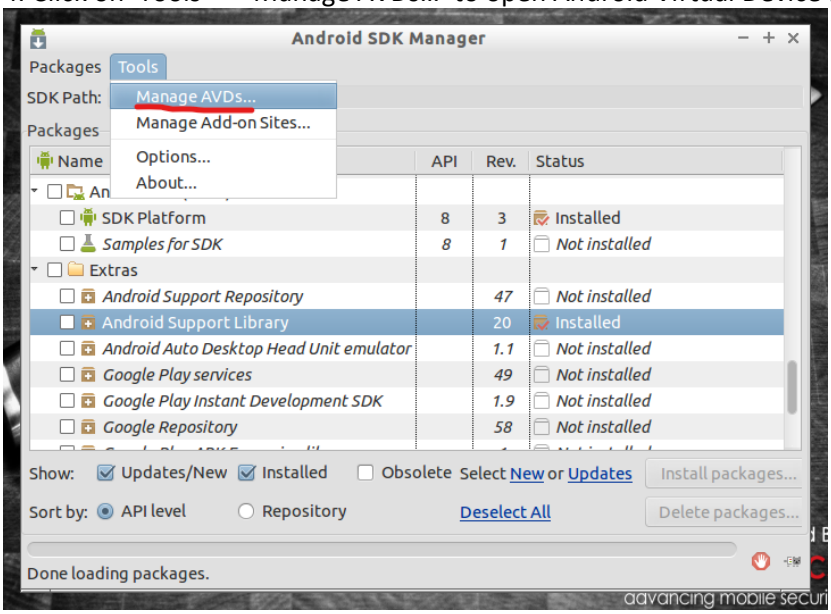


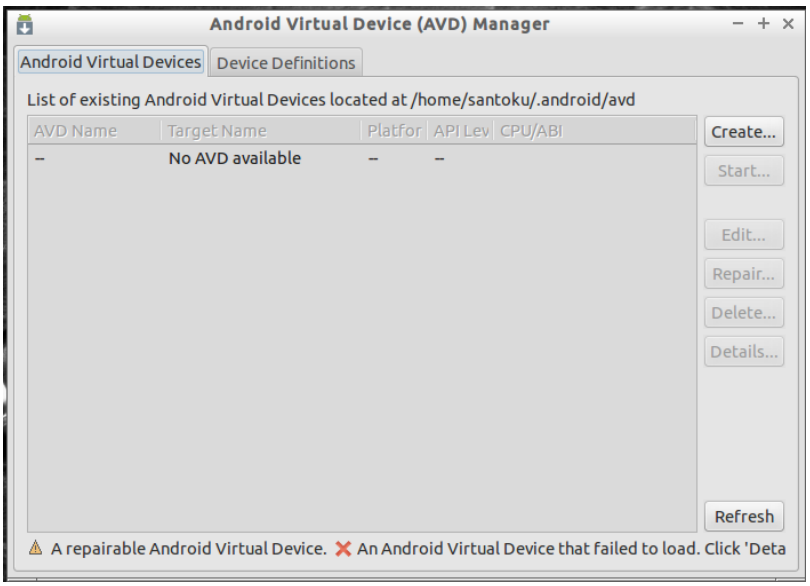
3. After opening the Android SDK Manager, install these four packages. (The virtual machine is installed with these packages, if yours do not have these packages, please install them as marked in the following images).



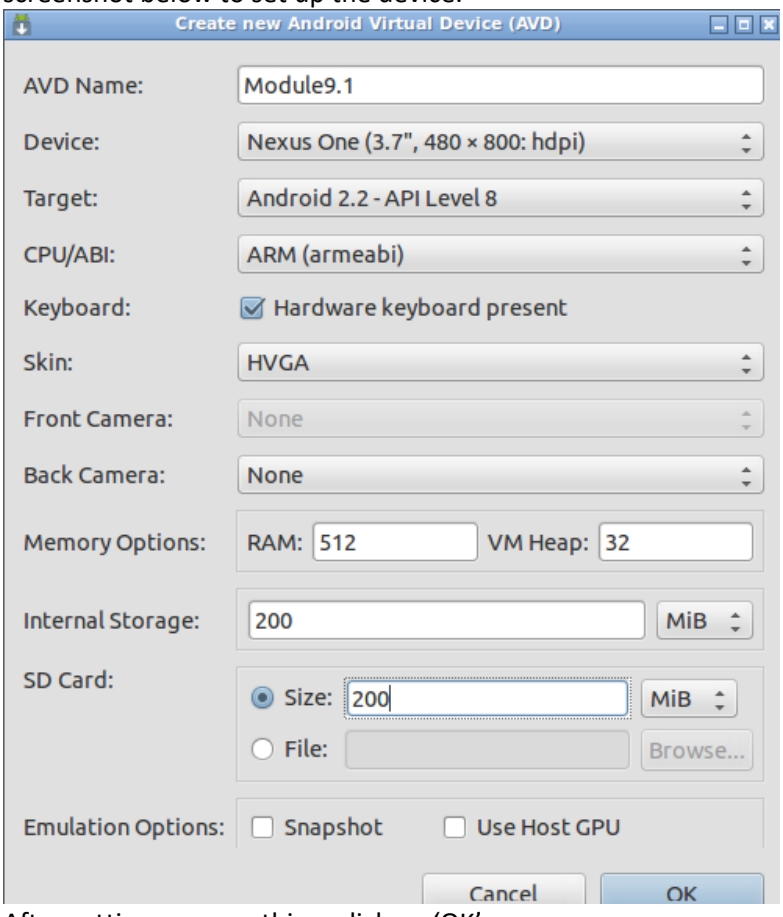


4. Click on ‘Tools’ -> ‘Manage AVDs…’ to open Android Virtual Device (AVD) Manager.



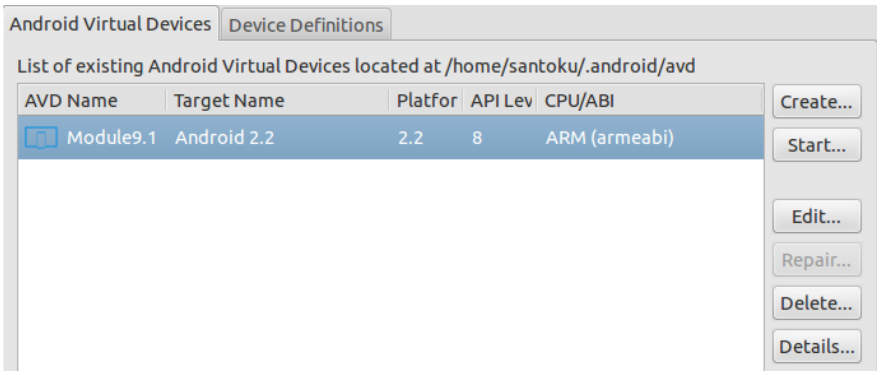


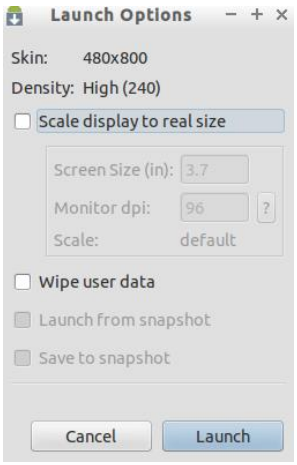
5. Then click on ‘Create’ on the right column to create a new Android Virtual Device. Follow the screenshot below to set up the device.



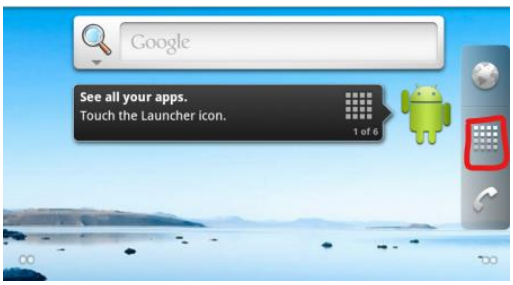
After setting up everything, click on ‘OK’.

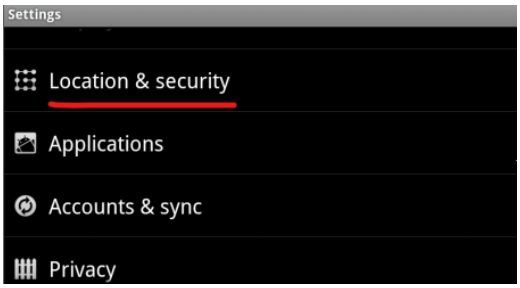
6. Click on the device and start the device. Set up the lunch option and then launch the device.

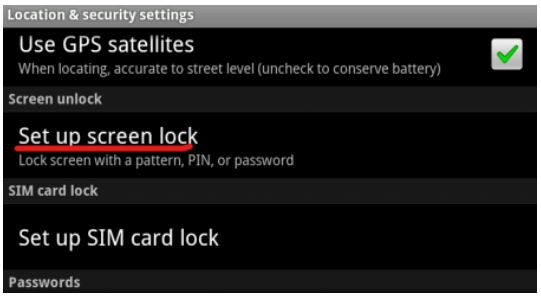


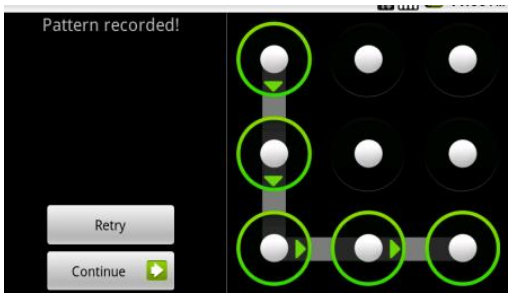


7. After opening the device, you can click the icon in the middle one. The choose the "Setting"-> "Location & Security" -> "Set up screen lock" and choose the "pattern" to set up a pattern password.

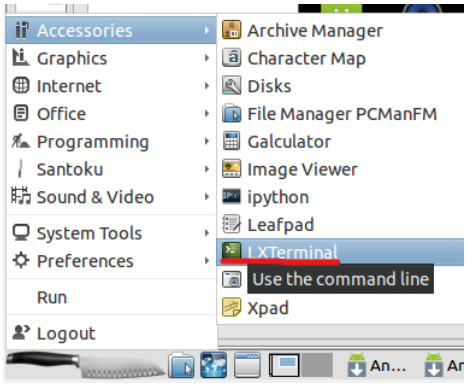








8. After setting up the pattern password, click the knife icon on the left button corner, choose "Accessories" → "LXTerminal" to open the terminal, and enter command ***adb shell*** to open the adb shell. (Note: If you cannot open the adb shell, you can enter the command **telnet localhost 5554**, and then enter **adb shell**).



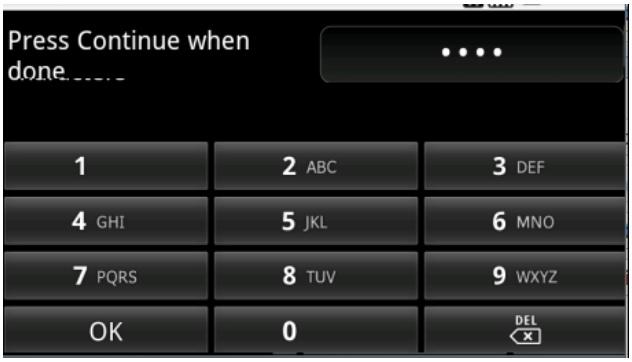

```
santoku@santoku-VirtualBox:~$ adb shell
```

9. After opening the adb shell, enter command ***cd data/system*** -> ***ls***. As shown in the screenshot, the file called gesture.key stored the gesture that we set before. Then enter command ***rm gesture.key*** to remove this file. In this way, the gesture password is deleted. Lastly, enter command ***ls gesture.key*** to make sure the file is deleted.

```
santoku@santoku-VirtualBox:~$ adb shell
# cd data/system
# ls
packages.list
packages.xml
appwidgets.xml
wallpaper_info.xml
batterystats.bin
usagestats
registered_services
entropy.dat
accounts.db
sync
dropbox
throttle
gesture.key
device_policies.xml
# rm gesture.key
# ls gesture.key
gesture.key: No such file or directory
#
```

10. After deleting the gesture.key file, go back to the lock screen by clicking the first button on the navigation bar. And enter any pattern to unlock the screen. As shown in the screenshot, even though the pattern is not correct, the screen can also be unlocked. Bypassing the lock screen is successful.

11. For the PIN password, using the same way can also bypass the lock screen. After setting the PIN, enter command ***ls data/system*** to find the password file. The file called password.key file contains the PIN password. Enter command ***rm password.key*** to remove the password. After removing the password, repeat the same process in step 13. Go back to the lock screen, the password is not needed, just slide the green lock, the screen will unlock.




```
# ls
device_policies.xml
password.key
packages.list
packages.xml
appwidgets.xml
wallpaper_info.xml
batterystats.bin
usagestats
registered_services
entropy.dat
accounts.db
sync
dropbox
throttle
# rm password.key
# ls password.key
password.key: No such file or directory
#
```

Deliverable:

You need to submit a lab report to Canvas. (You can submit a report with all the screenshots and questions for activity 8 in one file or you can submit several files for each module). Note: Your lab report should contain two parts.

1) Screenshots (3-4 screenshots in total for this module): Please take screenshots after you install the santoku virtual machine. Please take a screenshot of the Module9.1 virtual device (step 5). Then please take a screenshot after you finish step 9, please include the adb shell interface.

2) Please answer the following questions:

1. Which file contains the password that we set?

2. Where are the password files located?

3. Which command do we need to enter to open the adb shell in the terminal?

4. How to use the adb shell to bypass the lock screen?

5. After removing the password file, does the screen lock still exist?