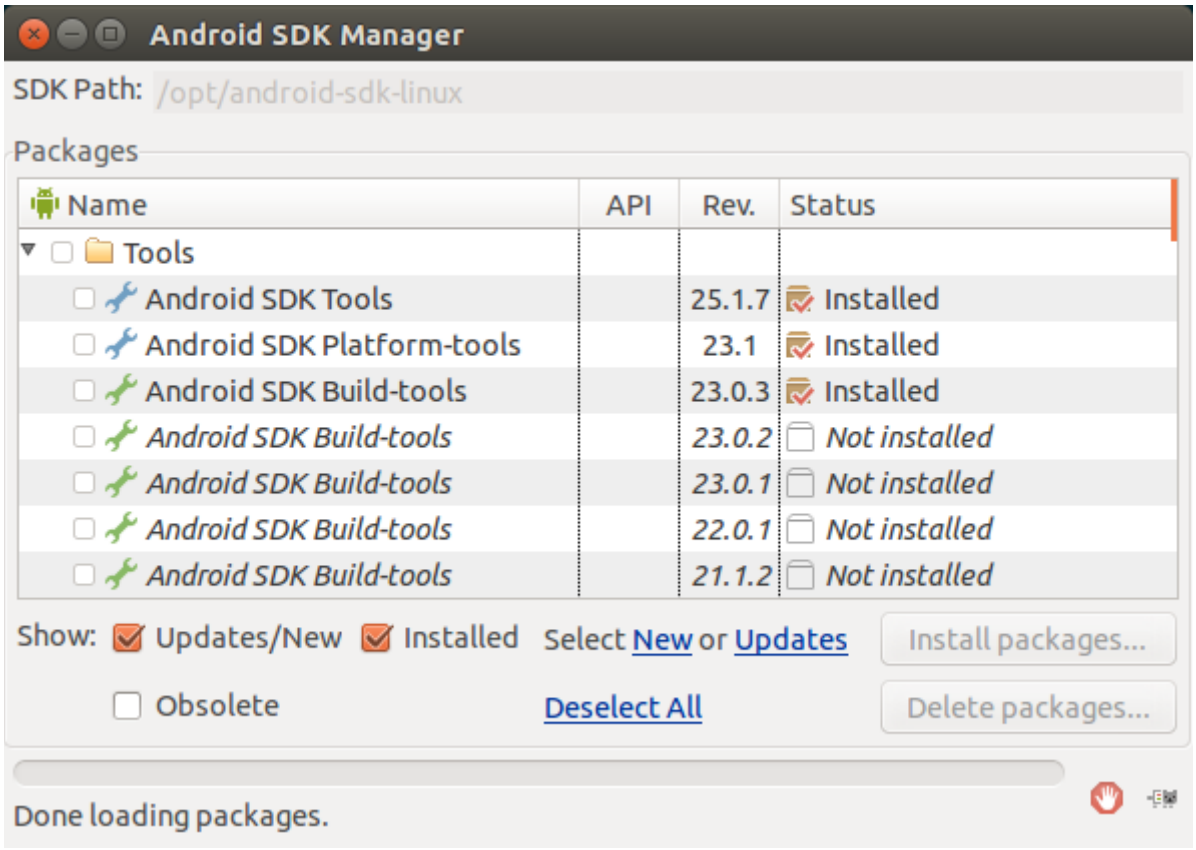
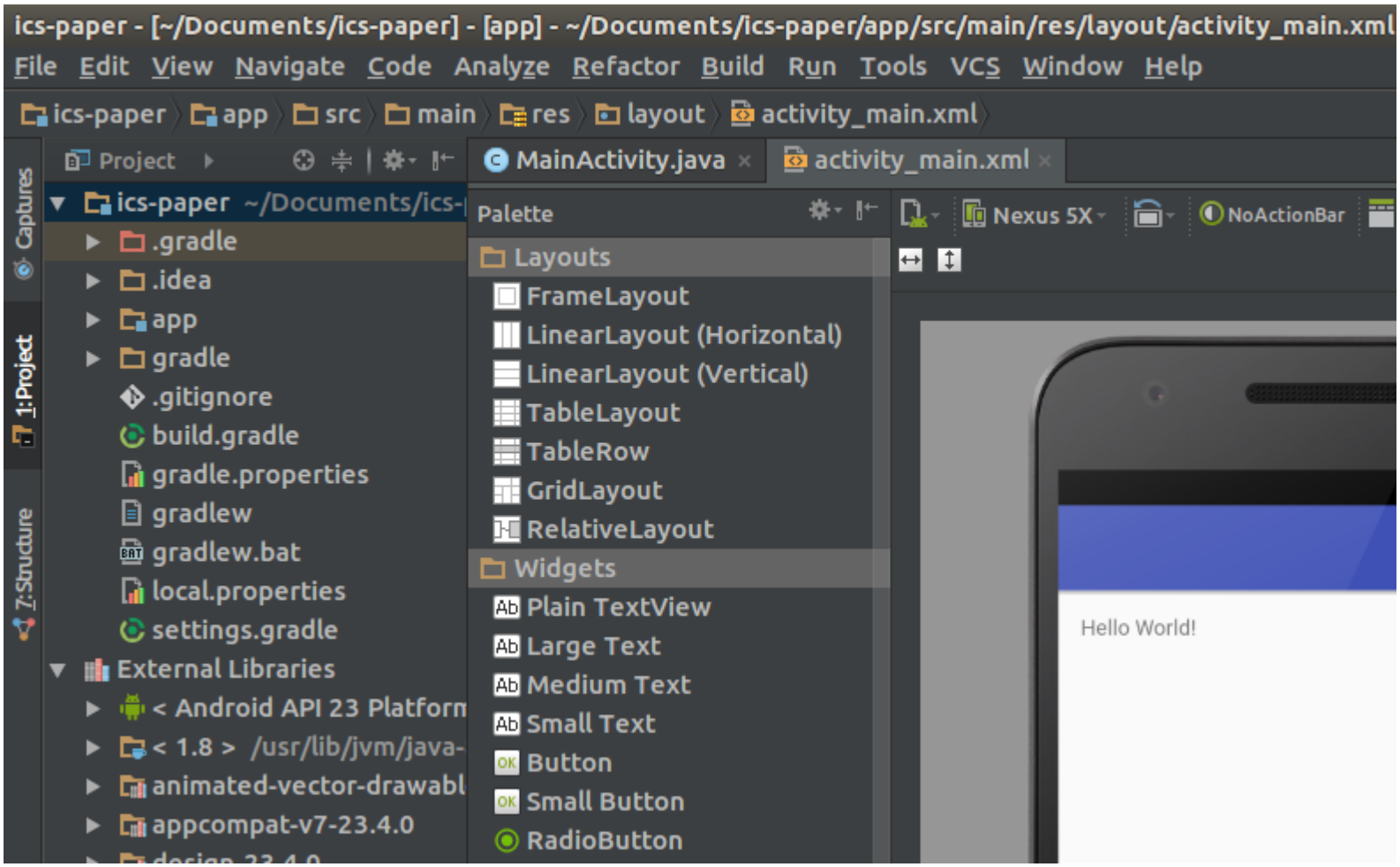
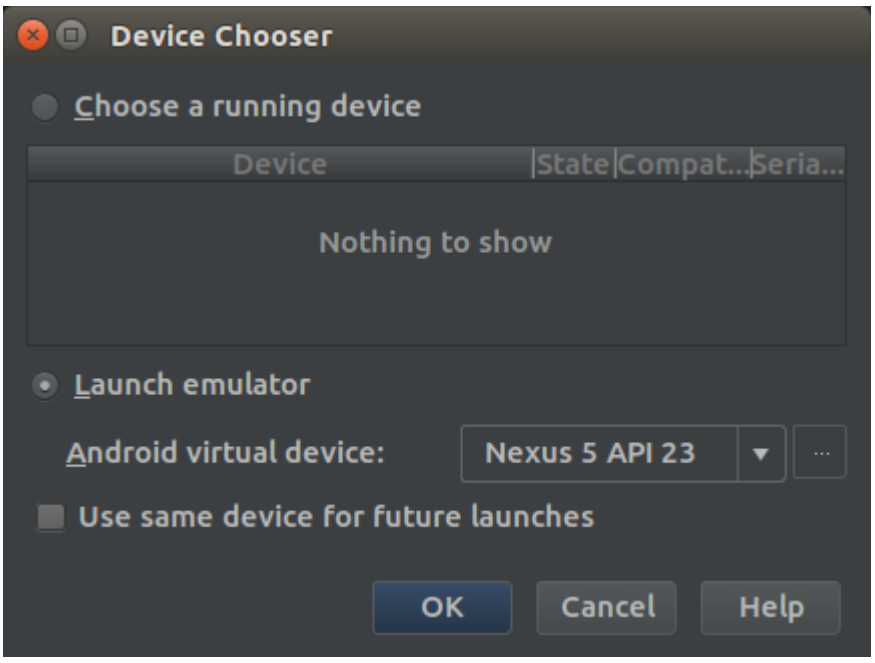
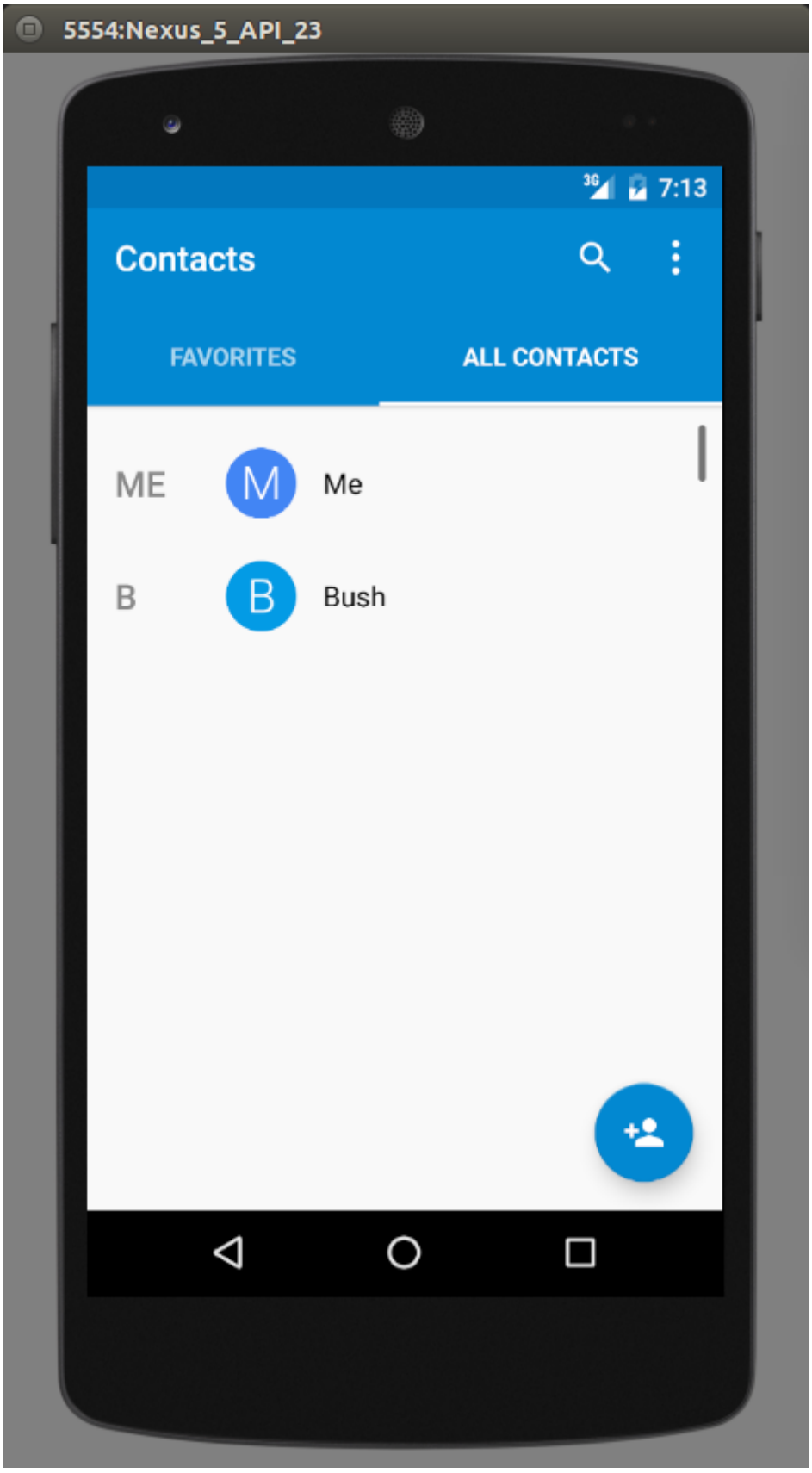
1. Android Debug Tool (i) Install Android SDK. (ii) Connect an Android device or emulator to the host which runs DDMS in the SDK. (iii) Dump and explain contents output by logcat in DDMS.

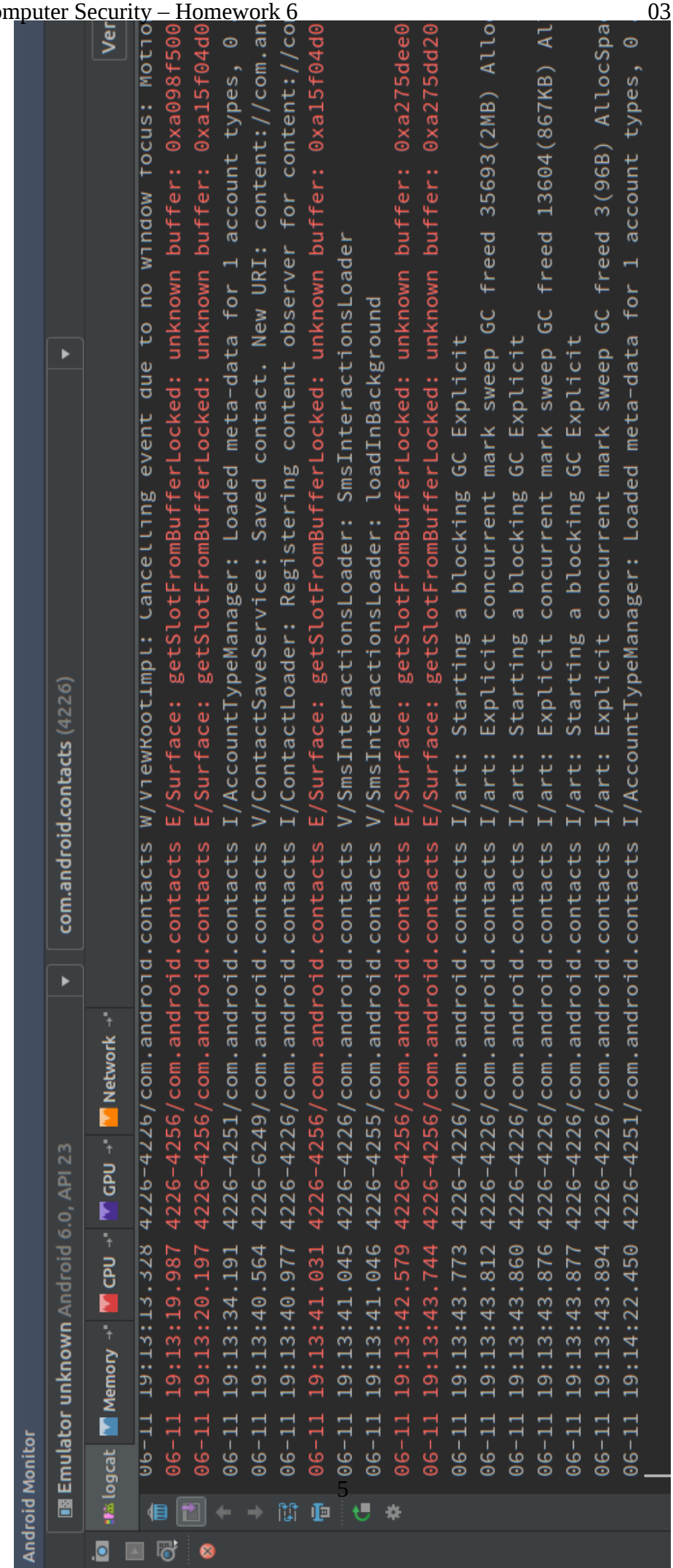


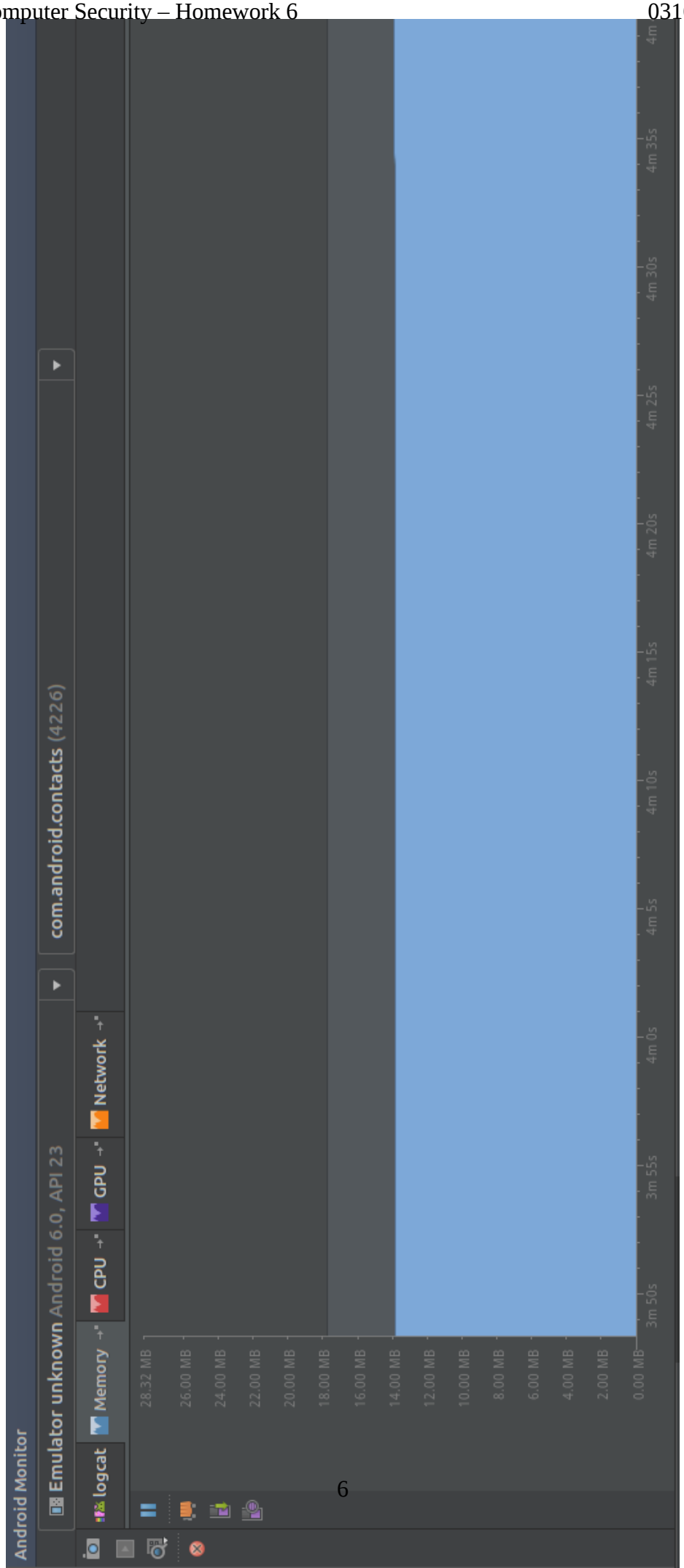

ics-paper - [~/Documents/ics-paper] - [app] - ~/Documents/ics-paper/app/src/main/res/layout/activity_main.xml
File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help
ics-paper app src main res layout activity_main.xml
Project
MainActivity.java
activity_main.xml
ics-paper ~/Documents/ics-
.gradle
.idea
app
gradle
.gitignore
build.gradle
gradle.properties
gradlew
gradlew.bat
local.properties
settings.gradle
External Libraries
< Android API 23 Platform
< 1.8 > /usr/lib/jvm/java-
animated-vector-drawabl
appcompat-v7-23.4.0
Palette
Layouts
FrameLayout
LinearLayout (Horizontal)
LinearLayout (Vertical)
TableLayout
TableRow
GridLayout
RelativeLayout
Widgets
Plain TextView
Large Text
Medium Text
Small Text
Button
Small Button
RadioButton
Nexus 5X
NoActionBar
Hello World!
Captures
1:Project
7:Structure


Device Chooser
Choose a running device
Device
State
Compat...
Seria...
Nothing to show
Launch emulator
Android virtual device:
Nexus 5 API 23
Use same device for future launches
OK
Cancel
Help

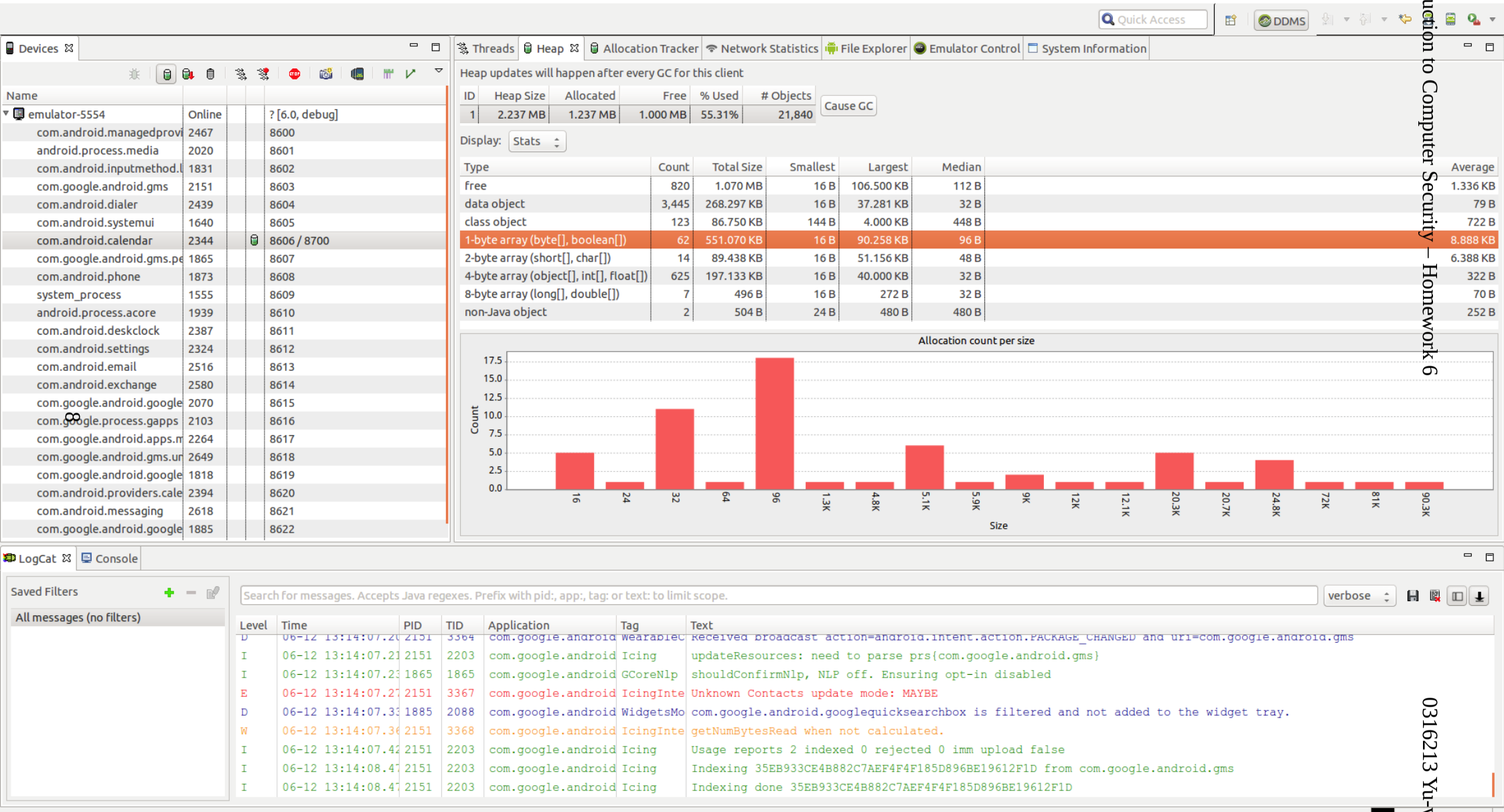

5554:Nexus_5_API_23
7:01
Google
Say "Ok Google"
Google
Play Games


5554:Nexus_5_API_23
7:13
Contacts
FAVORITES
ALL CONTACTS
ME
M
Me
B
B
Bush


Android Monitor
Emulator unknown Android 6.0, API 23
com.android.contacts (4226)
logcat
Memory
CPU
GPU
Network
06-11 19:13:13.328 4226-4226/com.android.contacts W/ViewRootImpl: Cancelling event due to no window focus: Motio
06-11 19:13:19.987 4226-4256/com.android.contacts E/Surface: getSlotFromBufferLocked: unknown buffer: 0xa098f500
06-11 19:13:20.197 4226-4256/com.android.contacts E/Surface: getSlotFromBufferLocked: unknown buffer: 0xa15f04d0
06-11 19:13:34.191 4226-4251/com.android.contacts I/AccountTypeManager: Loaded meta-data for 1 account types, 0
06-11 19:13:40.564 4226-6249/com.android.contacts V/ContactSaveService: Saved contact. New URI: content://com.an
06-11 19:13:40.977 4226-4226/com.android.contacts I/ContactLoader: Registering content observer for content://co
06-11 19:13:41.031 4226-4256/com.android.contacts E/Surface: getSlotFromBufferLocked: unknown buffer: 0xa15f04d0
06-11 19:13:41.045 4226-4226/com.android.contacts V/SmsInteractionsLoader: SmsInteractionsLoader
06-11 19:13:41.046 4226-4255/com.android.contacts V/SmsInteractionsLoader: loadInBackground
06-11 19:13:42.579 4226-4256/com.android.contacts E/Surface: getSlotFromBufferLocked: unknown buffer: 0xa275dee0
06-11 19:13:43.744 4226-4256/com.android.contacts E/Surface: getSlotFromBufferLocked: unknown buffer: 0xa275dd20
06-11 19:13:43.773 4226-4226/com.android.contacts I/art: Starting a blocking GC Explicit
06-11 19:13:43.812 4226-4226/com.android.contacts I/art: Explicit concurrent mark sweep GC freed 35693(2MB) Allo
06-11 19:13:43.860 4226-4226/com.android.contacts I/art: Starting a blocking GC Explicit
06-11 19:13:43.876 4226-4226/com.android.contacts I/art: Explicit concurrent mark sweep GC freed 13604(867KB) Al
06-11 19:13:43.877 4226-4226/com.android.contacts I/art: Starting a blocking GC Explicit
06-11 19:13:43.894 4226-4226/com.android.contacts I/art: Explicit concurrent mark sweep GC freed 3(96B) AllocSpa
06-11 19:14:22.450 4226-4251/com.android.contacts I/AccountTypeManager: Loaded meta-data for 1 account types, 0


Android Monitor
Emulator unknown Android 6.0, API 23
com.android.contacts (4226)
logcat
Memory
CPU
GPU
Network
28.32 MB
26.00 MB
24.00 MB
22.00 MB
20.00 MB
18.00 MB
16.00 MB
14.00 MB
12.00 MB
10.00 MB
8.00 MB
6.00 MB
4.00 MB
2.00 MB
0.00 MB
3m 50s
3m 55s
4m 0s
4m 5s
4m 10s
4m 15s
4m 20s
4m 25s
4m 30s
4m 35s
4m

→ Logcat has already been integrated into IntelliJ IDEA. Of course, we can still view it in an independent Android monitor. See the following screenshots.



0316213 Yu-wen Pwu

Search for messages. Accepts Java regexes. Prefix with pid:, app:, tag: or text: to limit scope.

Level	Time	PID	TID	Application	Tag	Text
D	06-12 13:18:56.001	2151	4945	com.google.android.gms	WearableController	Received broadcast action=android.intent.action.PACKAGE_CHA
D	06-12 13:18:56.005	1885	2088	com.google.android.goo	WidgetsModel	com.google.android.googlequicksearchbox is filtered and not
E	06-12 13:18:56.077	2151	4954	com.google.android.gms	IcingInternalCorpora	Unknown Contacts update mode: MAYBE
I	06-12 13:18:56.081	2151	2203	com.google.android.gms	Icing	updateResources: need to parse prs{com.google.android.gms}
W	06-12 13:18:56.201	2151	4957	com.google.android.gms	IcingInternalCorpora	getNumBytesRead when not calculated.
I	06-12 13:18:56.272	2151	4849	com.google.android.gms	CheckinUtil	Classify the device as Phone.
I	06-12 13:18:57.312	2151	2203	com.google.android.gms	Icing	Indexing 35EB933CE4B882C7AEF4F4F185D896BE19612F1D from com.g
I	06-12 13:18:57.317	2151	2203	com.google.android.gms	Icing	Indexing done 35EB933CE4B882C7AEF4F4F185D896BE19612F1D
I	06-12 13:19:00.701	1555	1569	system_process	ActivityManager	Waited long enough for: ServiceRecord{b1488e8 u0 com.google

→ There are tens of thousands of infos, warnings, errors, etc. produced by a single app.

2. Select an Android device or emulator (e.g. the one in Android SDK, Bluestacks, and so on), root it. It is recommended to root on an Android emulator to avoid turning your phones "bricked".

→ The adb shell is already rooted.

```
~ adb devices
List of devices attached
emulator-5554   device

~ adb shell
root@generic_x86:/ # su root
root@generic_x86:/ # whoami
root
root@generic_x86:/ # ls -al
drwxr-xr-x root     root              2016-06-11
drwxrwx--- system   cache             2016-06-11
lrwxrwxrwx root     root              1970-01-01
dr-x------ root     root              2016-06-11
lrwxrwxrwx root     root              2016-06-11
drwxrwx--x system   system            2016-06-11
-rw-r--r-- root     root          549 1970-01-01
```

→ If I want to gain root access inside the device, I still need to overwrite the default "su" program in the device. (See: http://stackoverflow.com/questions/5095234/how-to-get-root-access-on-android-emulator)

Here is the list of commands you have to run while the emulator is running, I test this solution for an avd on Android 2.2 :

```
adb shell mount -o rw,remount -t yaffs2 /dev/block/mtdblock03 /system
adb push su /system/xbin/su
adb shell chmod 06755 /system
adb shell chmod 06755 /system/xbin/su
```

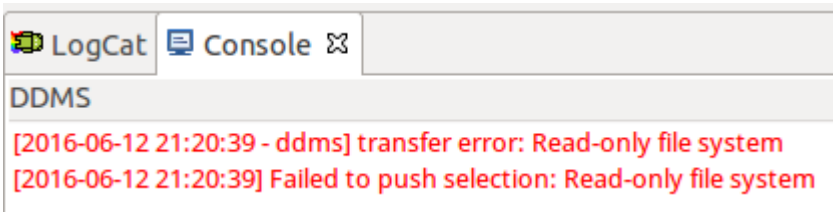
It assumes that the su binary is located in the working directory. You can find su and superuser here : http://forum.xda-developers.com/showthread.php?t=682828. You need to run these commands each time you launch the emulator. You can write a script that launch the emulator and root it.

share improve this answer edited Dec 3 '12 at 5:28 answered May 21 '11 at 21:02

a.b.d
1,536 ● 2 ● 19 ● 25

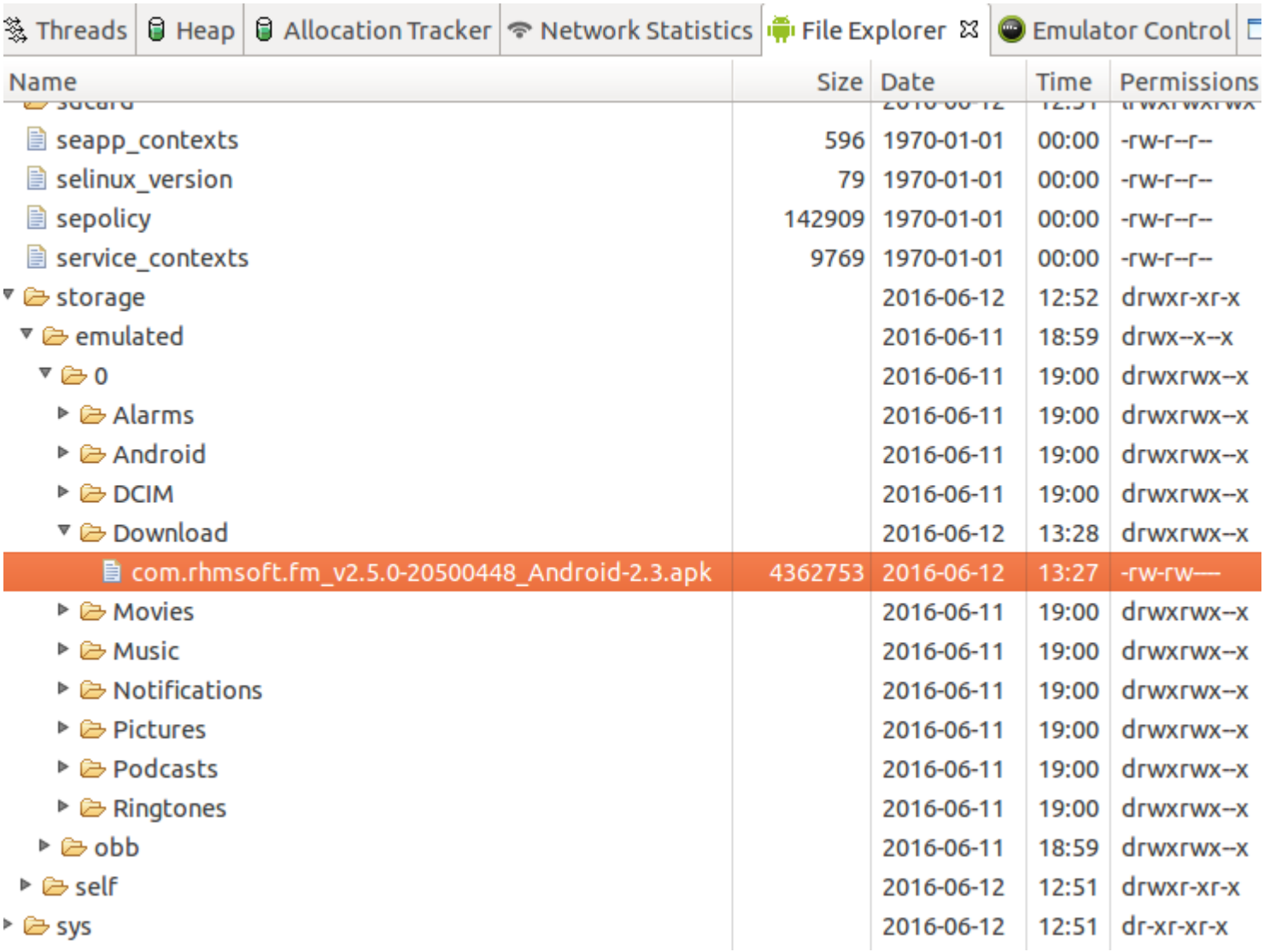
→ However, the system storage space in my virtual device is read-only. I have tried every possible solutions, but I still cannot make it writable. That's so strange…

```
~ adb root
adbd is already running as root
~ adb remount
remount succeeded
~ adb shell mount -o rw,remount -t yaffs2 /dev/block/mtdblock03 /system
mount: Read-only file system
~ adb push /bin/su /system/xbin/su
failed to copy '/bin/su' to '/system/xbin/su': Read-only file system
✗ ~ adb shell chmod 06755 /system
chmod: chmod '/system' to 46755: Read-only file system
~ sudo adb shell mount -o rw,remount -t yaffs2 /dev/block/mtdblock03 /system
[sudo] password for yuwen41200:
mount: Read-only file system
~ sudo adb push /bin/su /system/xbin/su
failed to copy '/bin/su' to '/system/xbin/su': Read-only file system
✗ ~ sudo adb remount
remount of /system failed: Read-only file system
remount failed
~ sudo adb shell chmod 06755 /system
chmod: chmod '/system' to 46755: Read-only file system
~
```

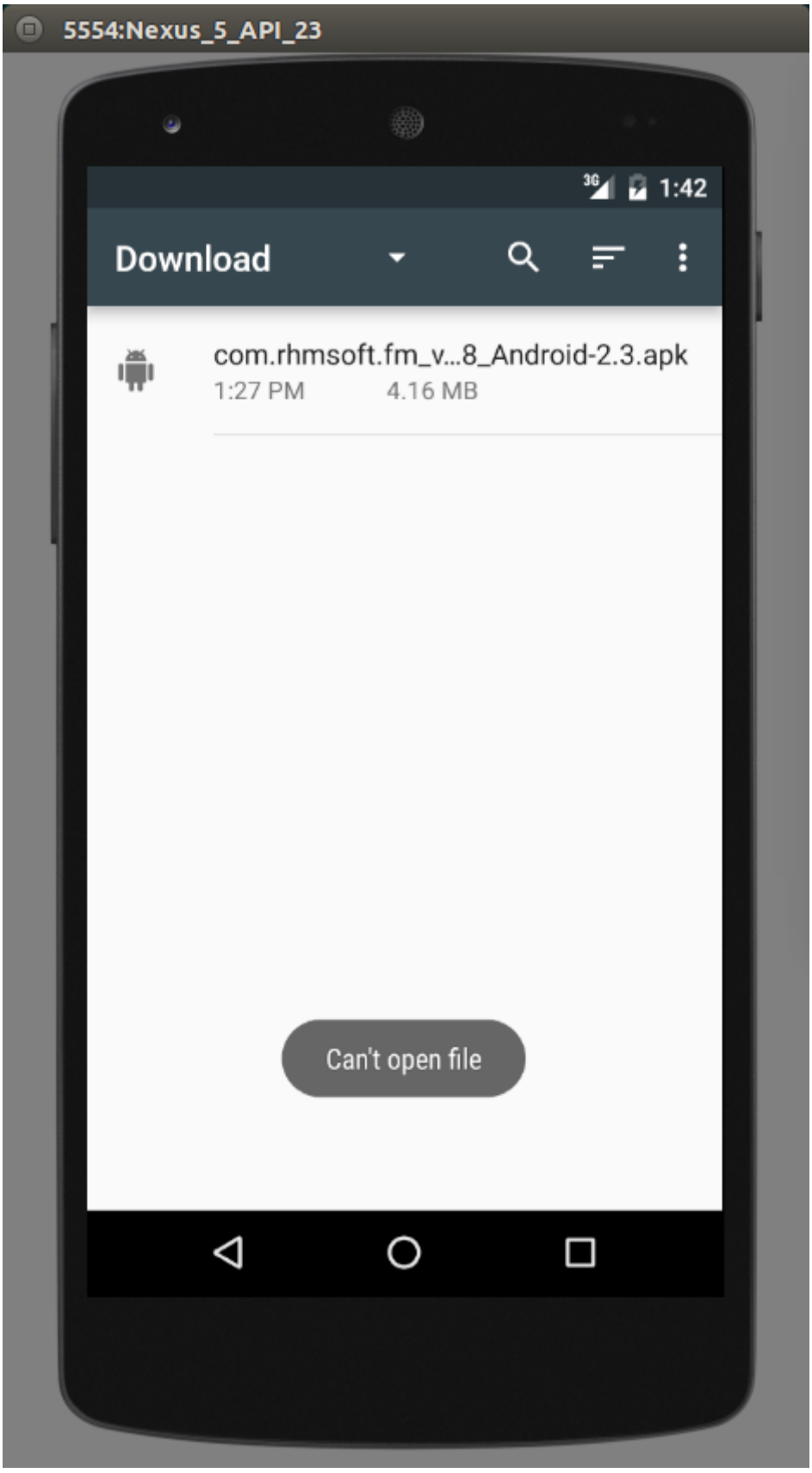


3. Use document management app (e.g. Root Explorer) to add/remove APK files to/from the folder "/system/app/" in a rooted Android device or emulator, and observe what happens.

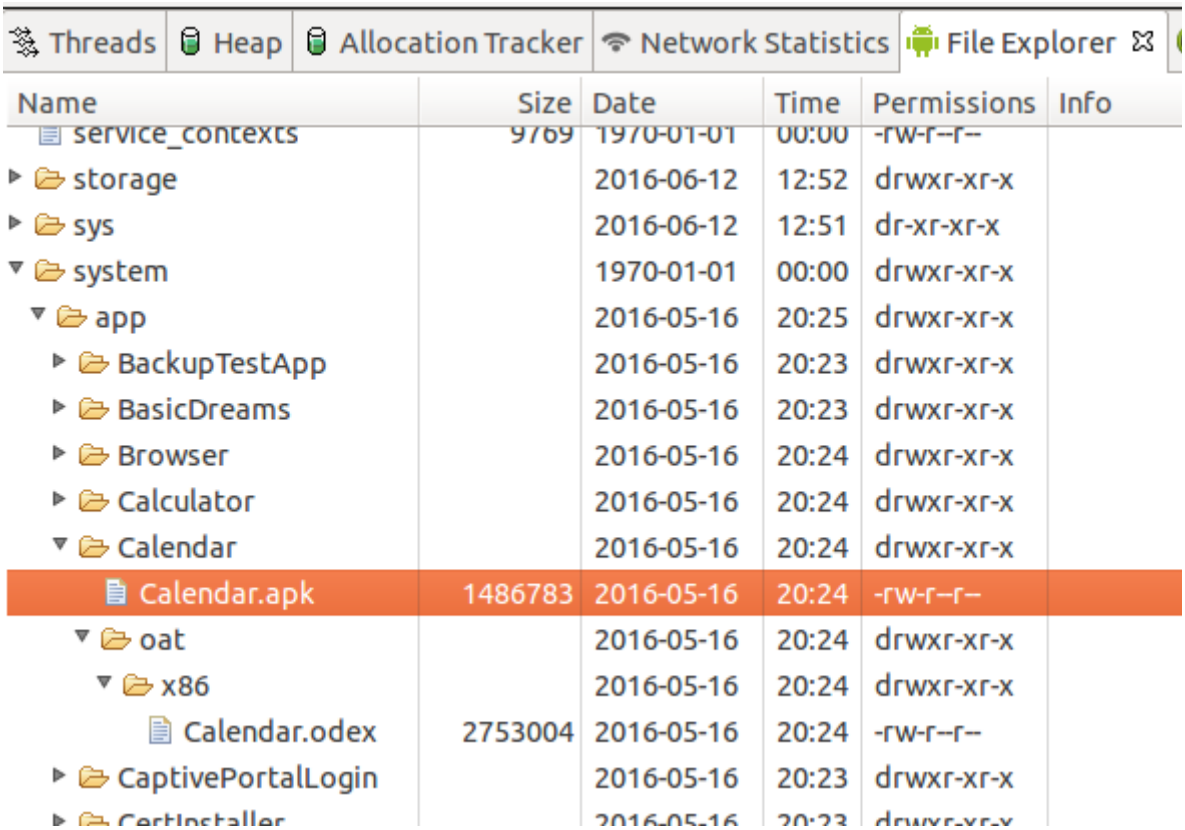
→ Since I cannot write to my system storage space directly, I tried to move the APK file to my SD card first, then install it.

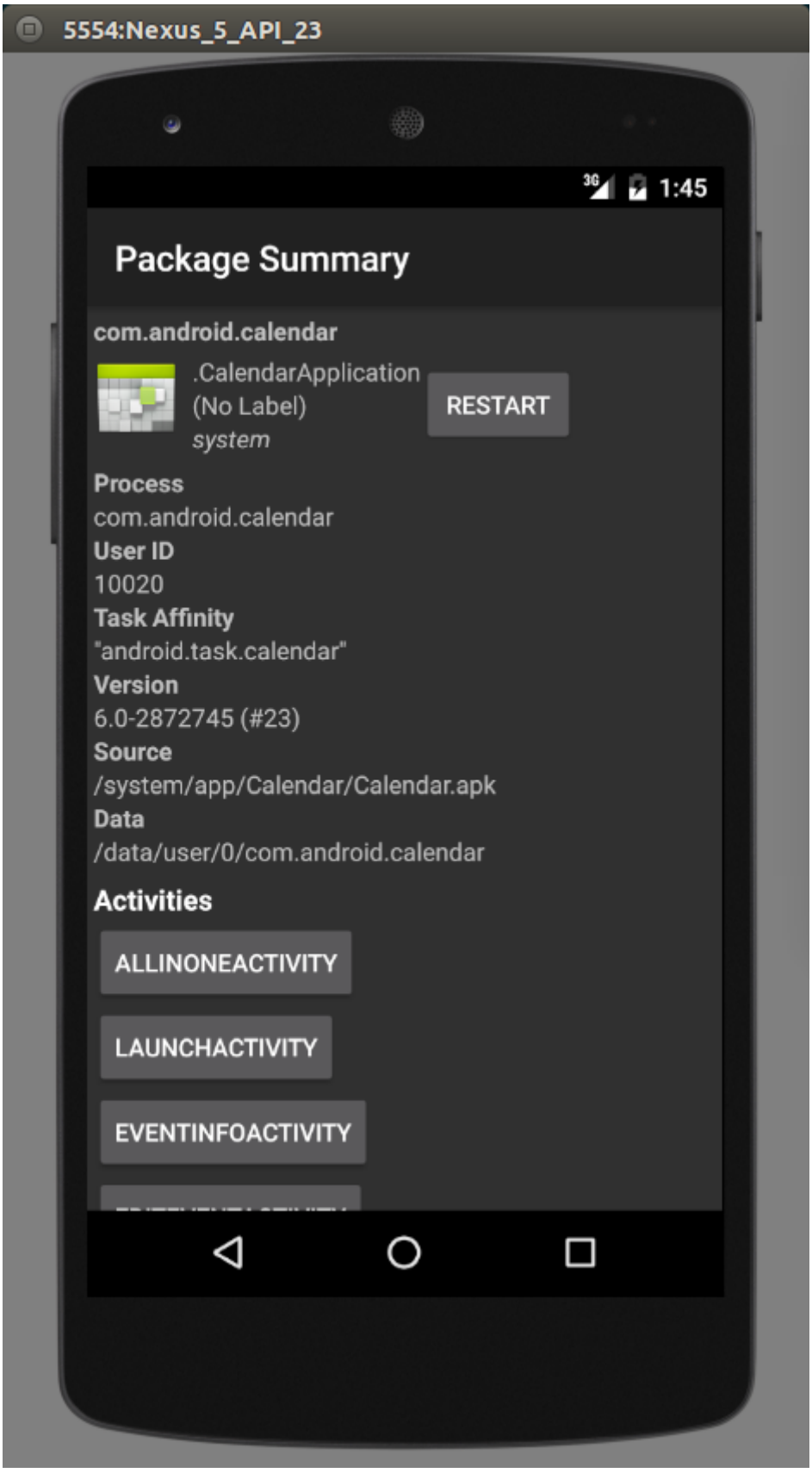


→ However, I failed to open the APK file in my device. (I have already enabled "installing apps from unknown sources.") I guess it's due to permission issues, but I have no way to modify its permission settings.


5554:Nexus_5_API_23
1:42
Download
com.rhmsoft.fm_v...8_Android-2.3.apk
1:27 PM 4.16 MB
Can't open file

→ Anyway, I know that all installed apps are stored in "/system/app/" and if I add/remove an APK file, the app is installed/removed. This can be observed from the following screenshots.



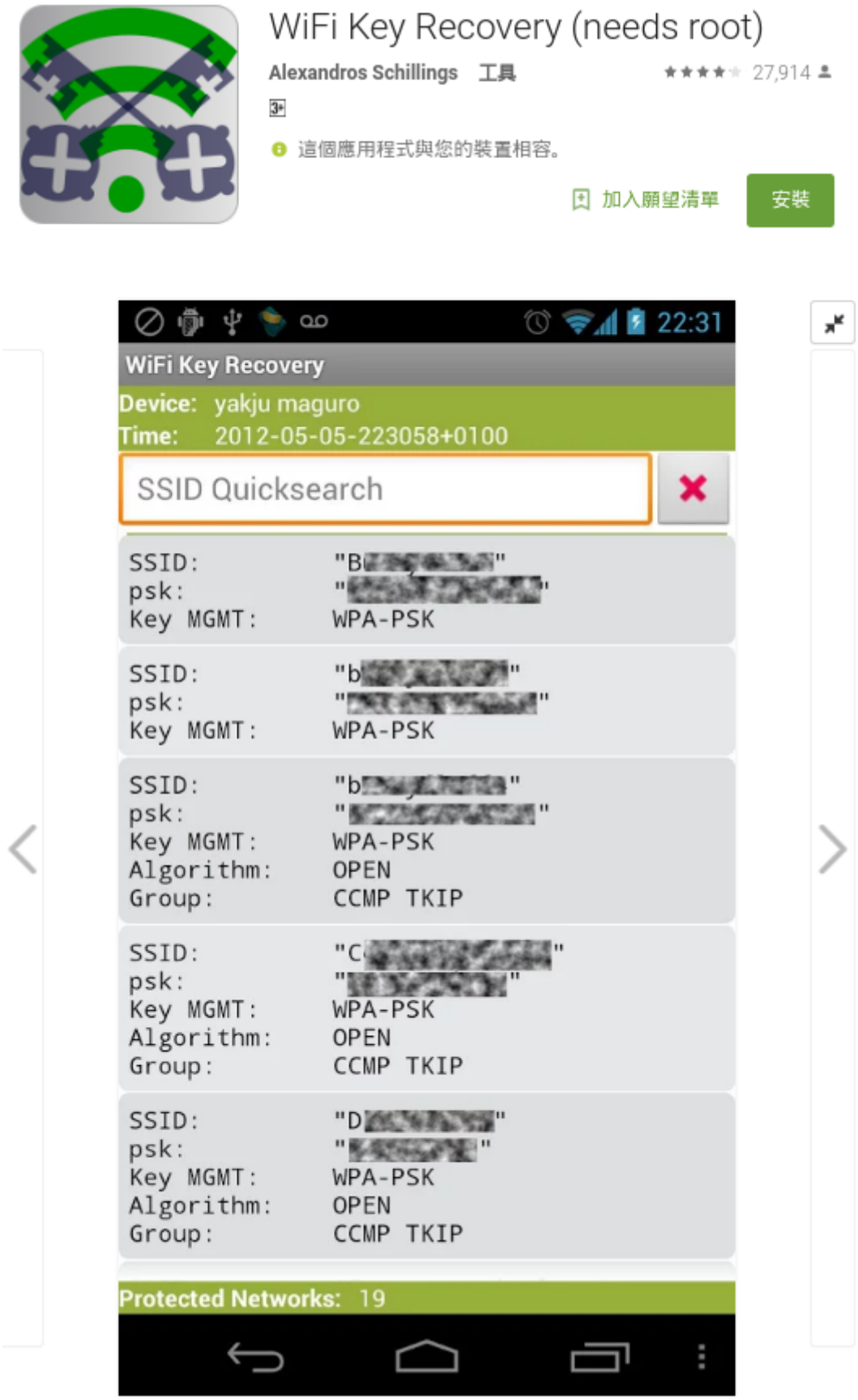

5554:Nexus_5_API_23
1:45
Package Summary
com.android.calendar
.CalendarApplication
(No Label)
system
RESTART
Process
com.android.calendar
User ID
10020
Task Affinity
"android.task.calendar"
Version
6.0-2872745 (#23)
Source
/system/app/Calendar/Calendar.apk
Data
/data/user/0/com.android.calendar
Activities
ALLINONEACTIVITY
LAUNCHACTIVITY
EVENTINFOACTIVITY

4. Install the app, AdBlock, in an rooted Android device or emulator and explain how it blocks Ads.

→ It works as a proxy. It filters all transmitted data. If the device is not rooted, it can only filter Wi-Fi data. Also, if the device is not rooted, users may need to set up the proxy by themselves.

5. Install a root-dependent app (except AdBlock) to a rooted Android device or emulator and explain why it needs a root system.

→ The "WiFi Key Recovery" app. It will show all Wi-Fi passwords stored in the device. It needs root privilege because it need to parse the "/data/misc/wifi/wpa_supplicant.conf" file. This file is only accessible for root.


WiFi Key Recovery (needs root)
Alexandros Schillings 工具
27,914
3+
這個應用程式與您的裝置相容。
加入願望清單
安裝
22:31
WiFi Key Recovery
Device: yakju maguro
Time: 2012-05-05-223058+0100
SSID Quicksearch
SSID: "B[redacted]"
psk: "[redacted]"
Key MGMT: WPA-PSK
SSID: "b[redacted]"
psk: "[redacted]"
Key MGMT: WPA-PSK
SSID: "b[redacted]"
psk: "[redacted]"
Key MGMT: WPA-PSK
Algorithm: OPEN
Group: CCMP TKIP
SSID: "C[redacted]"
psk: "[redacted]"
Key MGMT: WPA-PSK
Algorithm: OPEN
Group: CCMP TKIP
SSID: "D[redacted]"
psk: "[redacted]"
Key MGMT: WPA-PSK
Algorithm: OPEN
Group: CCMP TKIP
Protected Networks: 19

6. Select one version of iOS, survey how to jailbreak it, and list the steps.

→ For iOS 9.0.2, we can follow the steps in http://www.downloadpangu.org/pangu-9-download.html. To sum up:

(i) Back up all data in your iOS device.
(ii) Disable Find My iPhone , Touch ID and Passcode.
(iii) Connect your iOS device to your computer.
(iv) Run Pangu on your computer (as administrator), follow the instructions on your screen.
(v) Done.