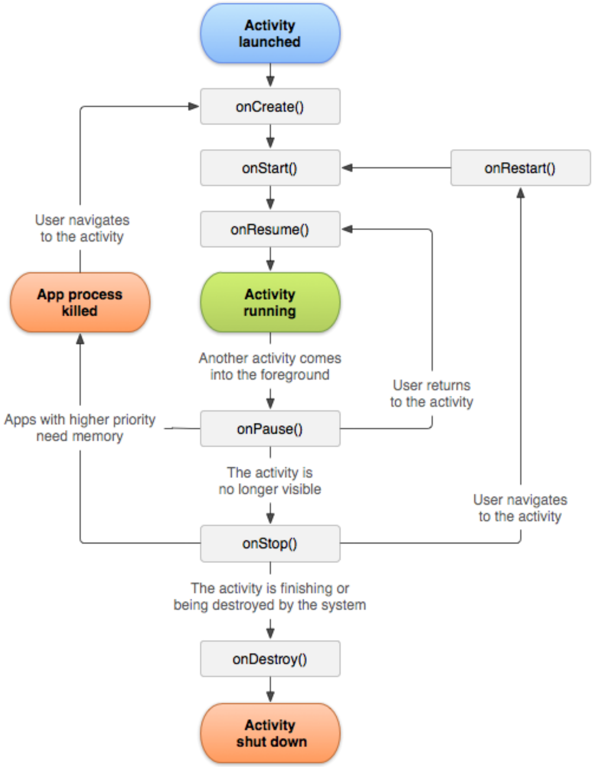
PROXMARK3 ON ANDROID PLATFORM

Lee Haw 2013/04/23

Brief Introduction of Android App

- Activity
  - "An **Activity** is an application component that provides a **screen** with which users can **interact** in order to do something."
- MVC
  - Model: ---
  - View: View
  - Controller: Activity

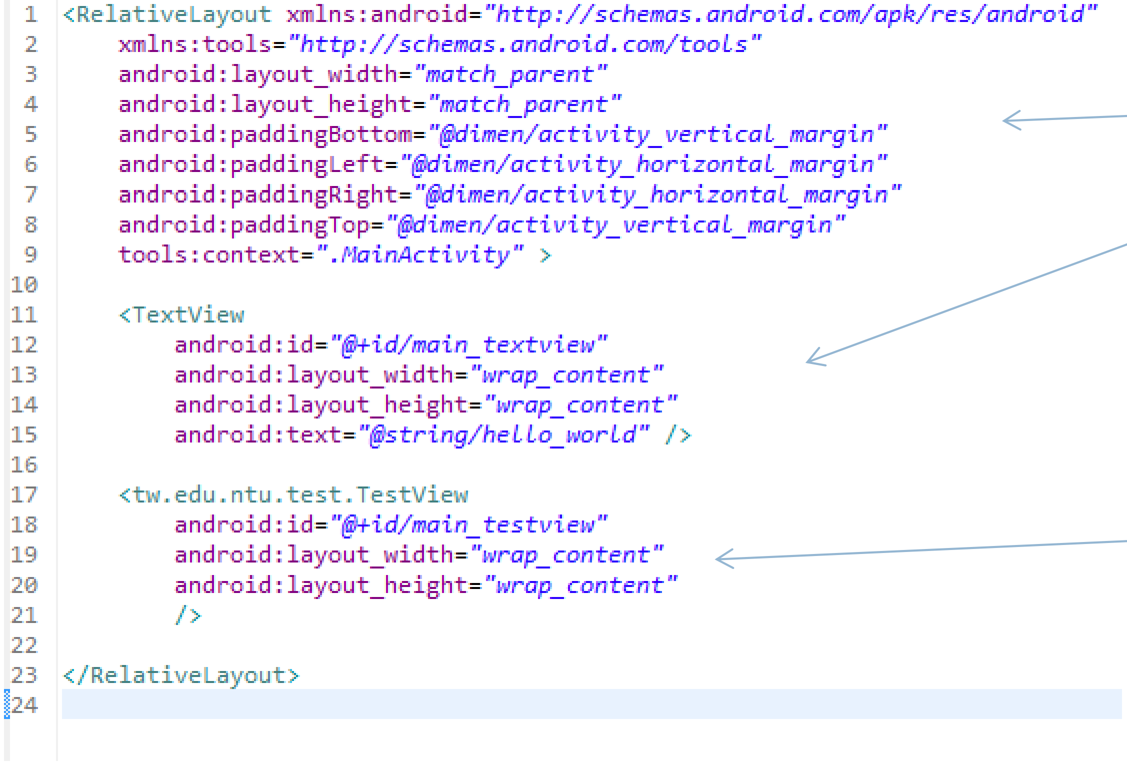

Activity launched
onCreate()
onStart()
onRestart()
User navigates to the activity
onResume()
App process killed
Activity running
Another activity comes into the foreground
User returns to the activity
Apps with higher priority need memory
onPause()
The activity is no longer visible
User navigates to the activity
onStop()
The activity is finishing or being destroyed by the system
onDestroy()
Activity shut down

Brief Introduction of Android App

- Background Service
  - Service, Thread, Handler, AsyncTask …
  - Using when we want to do some task which need lots of time.
    - Will not block the main thread (UI thread).
    - Ex:
      - Download data from server.
      - Complicate calculation.
      - Database read/write.

Brief Introduction of Android App

- UI component
  - Define in a Xml file
  - Example:



```
<RelativeLayout xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools"
    android:layout_width="match_parent"
    android:layout_height="match_parent"
    android:paddingBottom="@dimen/activity_vertical_margin"
    android:paddingLeft="@dimen/activity_horizontal_margin"
    android:paddingRight="@dimen/activity_horizontal_margin"
    android:paddingTop="@dimen/activity_vertical_margin"
    tools:context=".MainActivity" >

    <TextView
        android:id="@+id/main_textview"
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        android:text="@string/hello_world" />

    <tw.edu.ntu.test.TestView
        android:id="@+id/main_testview"
        android:layout_width="wrap_content"
        android:layout_height="wrap_content"
        />

</RelativeLayout>

```

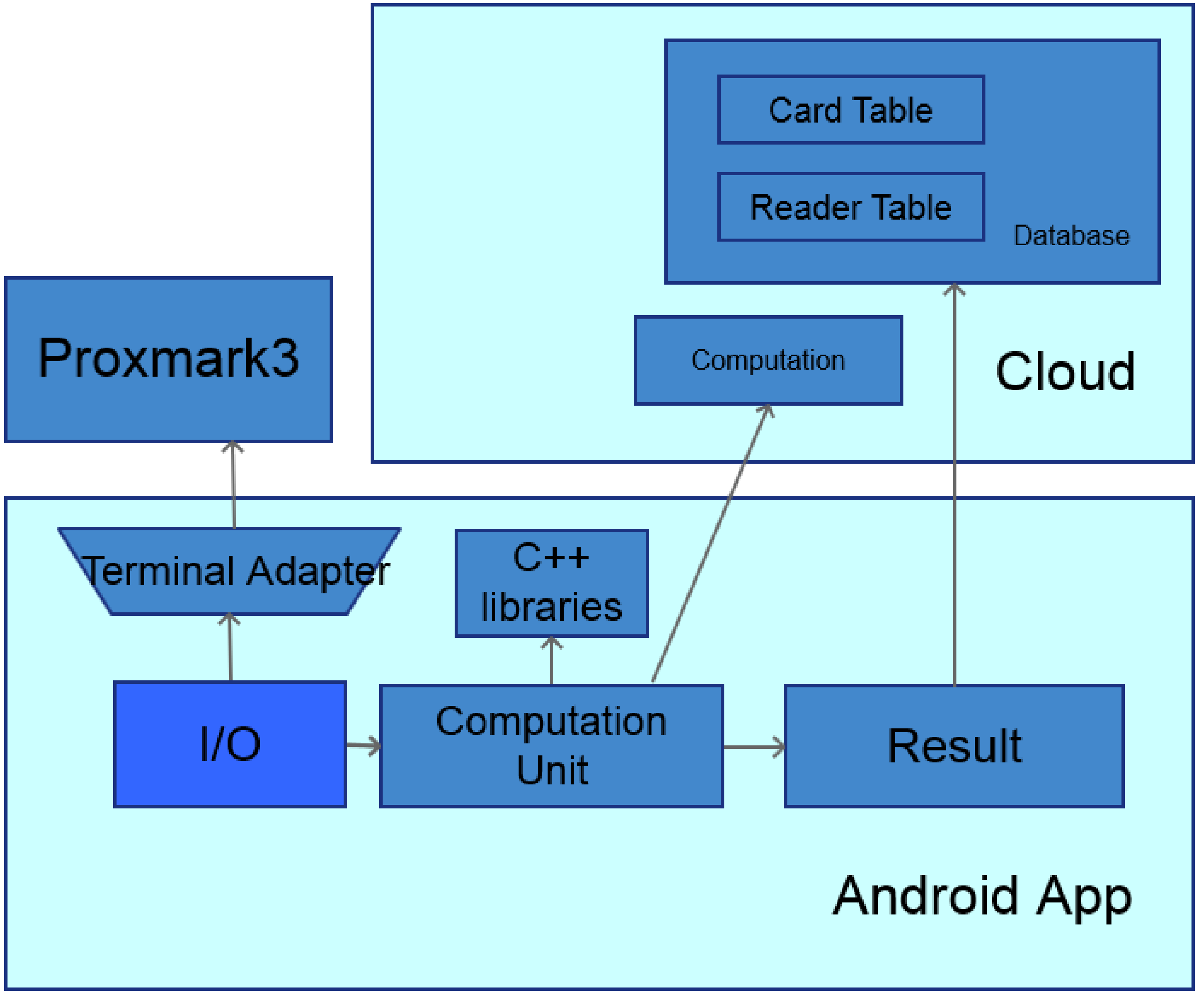
Built-in UI View

Custom View

Brief Introduction of Android App

- Some good tutorial for building android application.
  - Android Developer – API Guides
    - http://developer.android.com/guide/components/index.html
  - 深入淺出 Android
    - https://code.google.com/p/androidbmi/wiki/DiveIntoAndroid

Architecture



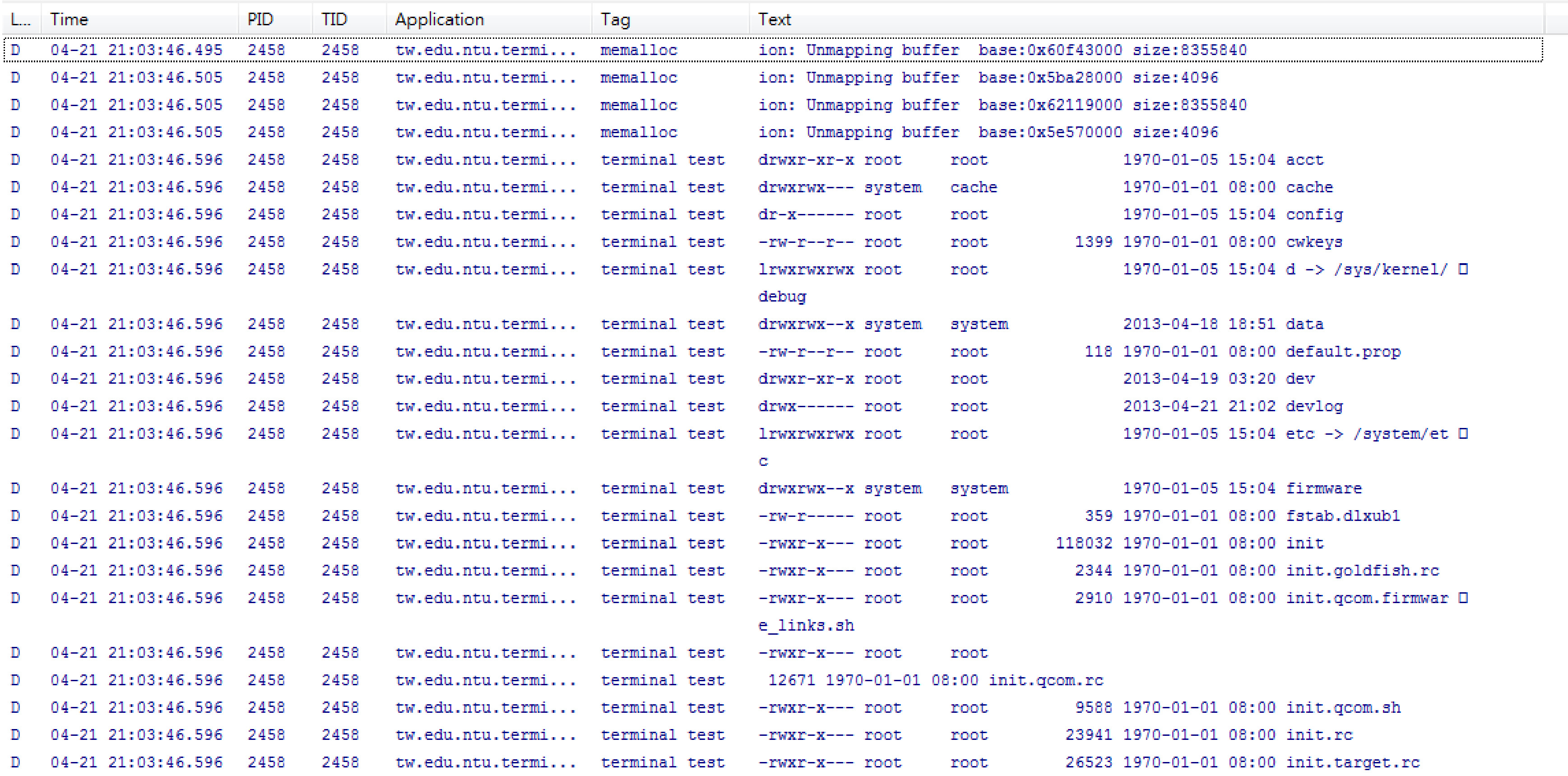
Terminal Interface

Terminal Interface

- Runtime runtime = Runtime.getRuntime();
- Process process = runtime.exec(cmd);
- InputStream is = process.getIntputStream();
- …

Terminal Interface

Result of “ls –l”



```
L...  Time                 PID    TID    Application         Tag             Text
D     04-21 21:03:46.495   2458   2458   tw.edu.ntu.termi... memalloc        ion: Unmapping buffer  base:0x60f43000 size:8355840
D     04-21 21:03:46.505   2458   2458   tw.edu.ntu.termi... memalloc        ion: Unmapping buffer  base:0x5ba28000 size:4096
D     04-21 21:03:46.505   2458   2458   tw.edu.ntu.termi... memalloc        ion: Unmapping buffer  base:0x62119000 size:8355840
D     04-21 21:03:46.505   2458   2458   tw.edu.ntu.termi... memalloc        ion: Unmapping buffer  base:0x5e570000 size:4096
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   drwxr-xr-x root     root               1970-01-05 15:04 acct
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   drwxrwx--- system   cache              1970-01-01 08:00 cache
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   dr-x------ root     root               1970-01-05 15:04 config
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   -rw-r--r-- root     root          1399 1970-01-01 08:00 cwkeys
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   lrwxrwxrwx root     root               1970-01-05 15:04 d -> /sys/kernel/ □
                                                                             debug
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   drwxrwx--x system   system             2013-04-18 18:51 data
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   -rw-r--r-- root     root           118 1970-01-01 08:00 default.prop
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   drwxr-xr-x root     root               2013-04-19 03:20 dev
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   drwx------ root     root               2013-04-21 21:02 devlog
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   lrwxrwxrwx root     root               1970-01-05 15:04 etc -> /system/et □
                                                                             c
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   drwxrwx--x system   system             1970-01-05 15:04 firmware
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   -rw-r----- root     root           359 1970-01-01 08:00 fstab.dlxub1
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   -rwxr-x--- root     root        118032 1970-01-01 08:00 init
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   -rwxr-x--- root     root          2344 1970-01-01 08:00 init.goldfish.rc
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   -rwxr-x--- root     root          2910 1970-01-01 08:00 init.qcom.firmwar □
                                                                             e_links.sh
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   -rwxr-x--- root     root
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test    12671 1970-01-01 08:00 init.qcom.rc
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   -rwxr-x--- root     root          9588 1970-01-01 08:00 init.qcom.sh
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   -rwxr-x--- root     root         23941 1970-01-01 08:00 init.rc
D     04-21 21:03:46.596   2458   2458   tw.edu.ntu.termi... terminal test   -rwxr-x--- root     root         26523 1970-01-01 08:00 init.target.rc
```

Terminal Interface

- Now I can get:
- proxmark3>
- And make sure whether the device found the proxmark3 or not.

Native Library

C++ Libraries

- Android NDK
  - The NDK is a toolset that **allows you to implement parts of your app using native-code languages** such as C and C++. For certain types of apps, this can be helpful so you can reuse existing code libraries written in these languages, but most apps do not need the Android NDK.
    - The NDK includes a set of cross-toolchains (compilers, linkers, etc..) that can generate native ARM binaries on Linux, OS X, and Windows (with Cygwin) platforms.
  - http://developer.android.com/tools/sdk/ndk/index.html
    - Full-guide

Proxmark3 on Android

Proxmark3 on Android

- Environment:
  - Windows-7 64bits
  - Nexus 7
    - 4.2.1
- Equipment:
  - OTG line (micro slave – USB master)
  - USB hub (only support USB2.0 interface)
- Apps (from Google Play):
  - Root Checker (Optional)
  - Android Terminal Emulator

Proxmark3 on Android

- 1. enable `Developer Mode`
  - Go to setting page => About tablet => click Build number 7 times => then the `Developer options` is available.
  - Go to `Developer options` => enable `USB debugging`
  - Note that your PC will install drivers for your device automatically.

Proxmark3 on Android

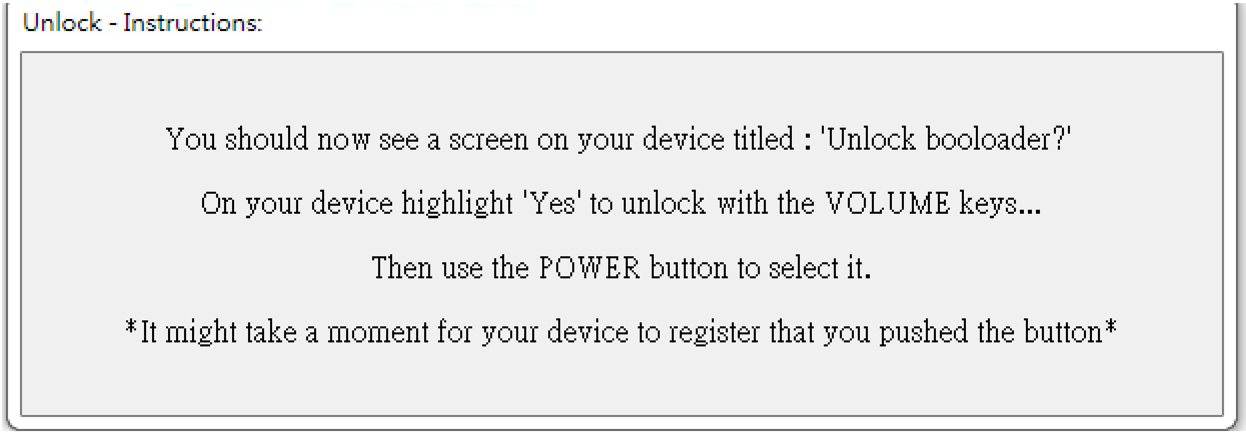
- 2. Unlock and root the android device:
  - Download Nexus Root Toolkit (I was using NRT_v1.6.3.sfx.exe, maybe others will work, too)
    - https://dl.dropboxusercontent.com/u/35314157/NRT_v1.6.3.sfx.exe
  - Install and open it, follow the guide and the toolkit will help you to root your device.
  - I'll record my steps and some matters needing attention in following.

Proxmark3 on Android

- 2. Unlock and root the android device:
  - Click: Full Drivers Installation Guide.
  - Launch Device Manager => uninstall Nexus7 driver
  - Unplug device => Launch USBView => uninstall all `Android ADB Interface` and all drivers comes from Google Inc.
  - Plug device back, it will install the drivers you need automatically.
  - Go to step 3 => full driver test
    - I'll retry it about 5 times to pass the test. (press OK when the warning comes up)
  - Finished Driver Test.
  - I use the USB hub and the transfer line for android, so that it will be forced to use USB2.0 interface.
  - Reboot device if it is in the bootloader mode.

Proxmark3 on Android

- 2. Unlock and root the android device:
  - Click Unlock.
  - After you see this, click the POWER key to choose YES.



Unlock - Instructions:

You should now see a screen on your device titled : 'Unlock booloader?'

On your device highlight 'Yes' to unlock with the VOLUME keys...

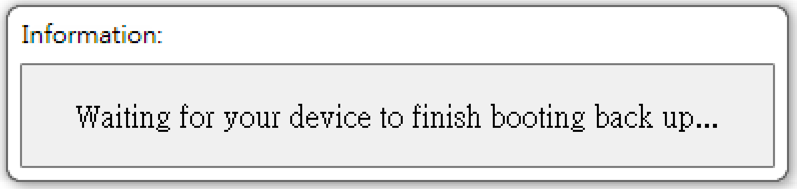
Then use the POWER button to select it.

It might take a moment for your device to register that you pushed the button

  - NOTE: It will wipe all data, so you need to enable developer mode again.

Proxmark3 on Android

- 2. Unlock and root the android device:
  - Click Root
  - It will show “Waiting for your device to finish booting backup… “
    - If it halt at this notification with a long time, click POWER button to reboot the device.
    - But it will fail after all



Information:

Waiting for your device to finish booting back up...

    - Retry it again and again, it will finish successfully.
    - NOTE: DO NOT disconnect the device when the toolkit is rooting your phone.
    - NOTE: Download “root checker” from Google Play to confirm you root it successful.

Proxmark3 on Android

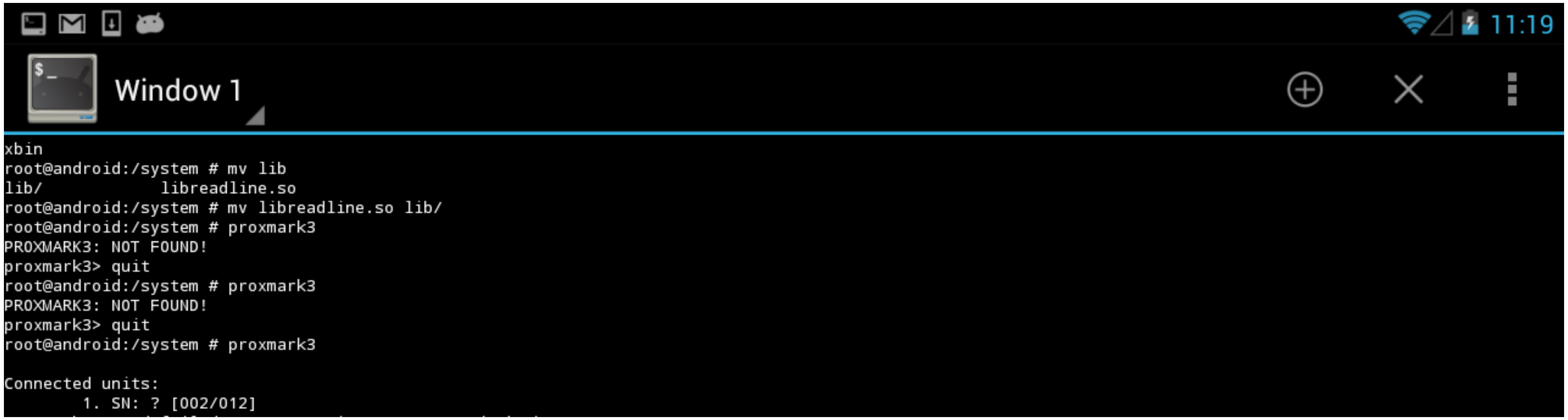
- 3. Build proxmark3's library
  - Follow this guide:
    - http://www.freebuf.com/tools/7244.html
    - The library files and executable file are:
      - https://dl.dropboxusercontent.com/u/35314157/libreadline.so
      - https://dl.dropboxusercontent.com/u/35314157/libreadline.so
      - https://dl.dropboxusercontent.com/u/35314157/libusb.so
      - https://dl.dropboxusercontent.com/u/35314157/proxmark3
    - Put them into the SD card of your device.

Proxmark3 on Android

- 3. Build proxmark3’s library
  - Open Terminal Emulator app:
  - Follow this guide to remount the /system
    - http://www.ourunix.org/post/166.html
    - In my case, I typed:
      - su
      - mount
      - mount –o remount /dev/block/platform/sdhci-tegra.3/by-name/APP /system
      - cd system
      - chmod 777 lib
      - chmod 777 bin
      - dd if=/sdcard/libusb.so of=/system/lib/libusb.so
      - dd if=/sdcard/libreadline.so of=/system/lib/libreadline.so
      - dd if=/sdcard/libtermcap.so of=/system/lib/libtermcap.so
      - dd if=/sdcard/proxmark3 of=/system/bin/proxmark3

Proxmark3 on Android

- 4. Connect proxmark3 and android phone:
  - Phone – OTG line – USB hub – proxmark3
  - Enter proxmark3 in the terminal.
  - It shows and works:



```
xbin
root@android:/system # mv lib
lib/            libreadline.so
root@android:/system # mv libreadline.so lib/
root@android:/system # proxmark3
PROXMARK3: NOT FOUND!
proxmark3> quit
root@android:/system # proxmark3
PROXMARK3: NOT FOUND!
proxmark3> quit
root@android:/system # proxmark3

Connected units:
        1. SN: ? [002/012]
```