

# COMP444 Workshop 4: Android Security

Daoyuan

Mar 28, 2014

# Objectives

- Learn to use basic Android analysis tools;
- Understand several flaws in Android apps;
- Practice to identify vulnerabilities in real-world Android apps.

Learn Android Tools

# **PART I: LEARN ANDROID TOOLS**

# Before we start ...

- Enter into **XP** using your lab machines.
- Android SDK tools are installed at:
  - **Y:\Win32\android-sdk-windows**
  - Later I will use **android-sdk-windows** for short
- Know how to use Windows **command line**:
  - Start → Run → Cmd

# Overview of Basic Android Tools

Android SDK includes a variety of tools.

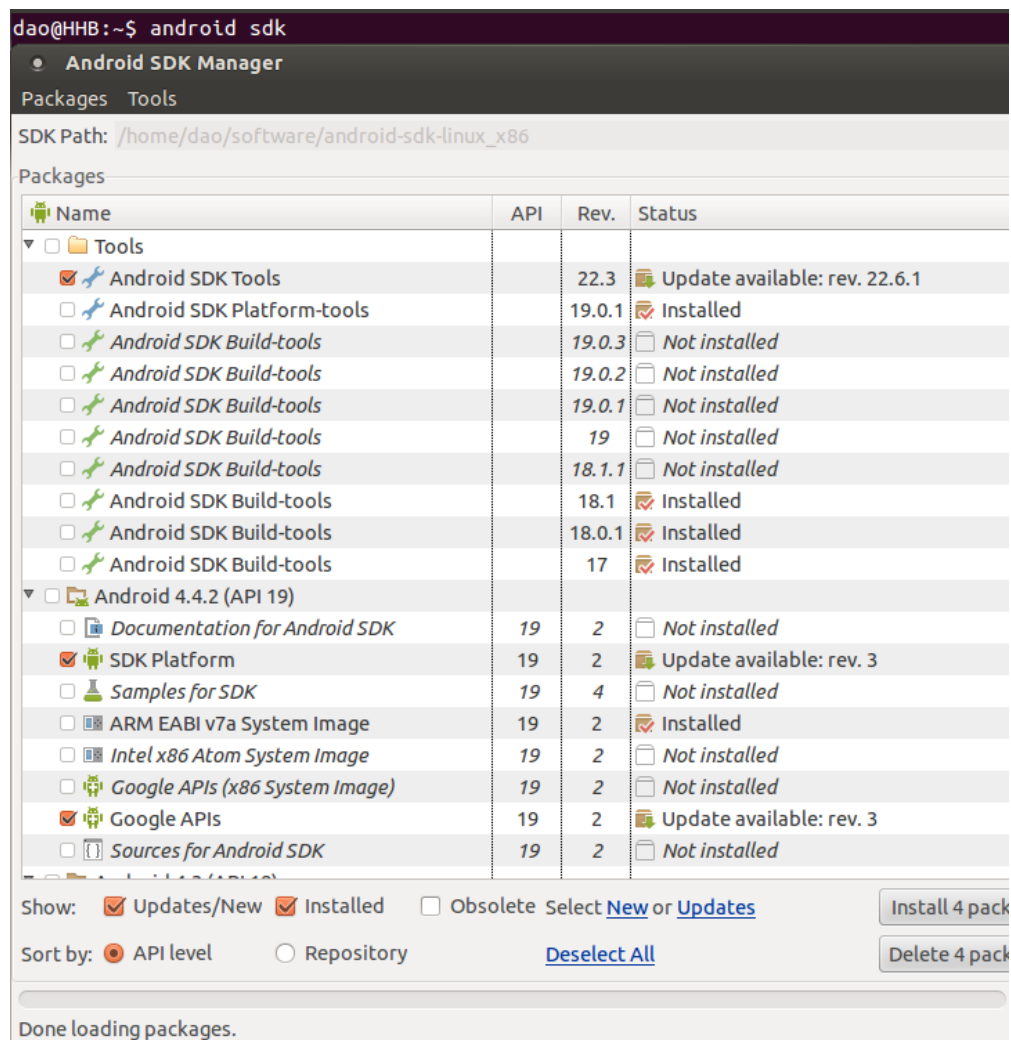
<http://developer.android.com/tools/help/index.html>

<http://developer.android.com/sdk/index.html>

- Android SDK Manager (android sdk)
  - Manage the installed components of the SDK.
- AVD Manager (android avd)
  - Manage your created emulator configurations.
- Emulator (emulator)
  - A QEMU-based device-emulation tool.
- Android Debug Bridge (adb)
  - Communicate with an emulator instance.
- Dalvik Debug Monitor Server (ddms) or (monitor)
  - Contain a set of useful tools to monitor Android apps.

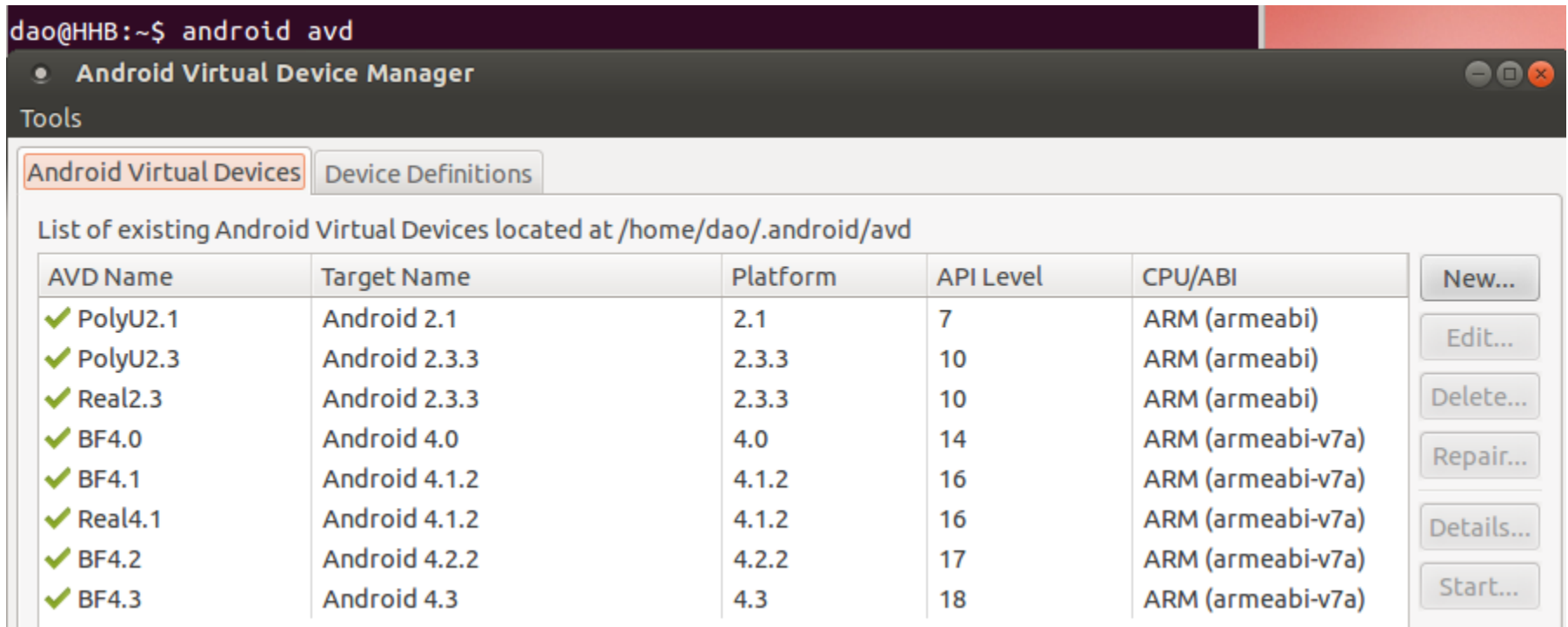
# Android SDK Manager (android sdk)

- Windows:
  - SDK Manager.exe
  - Quite slow ...
  - So avoid to open it.
- Major Android SDKs have been installed in the lab.



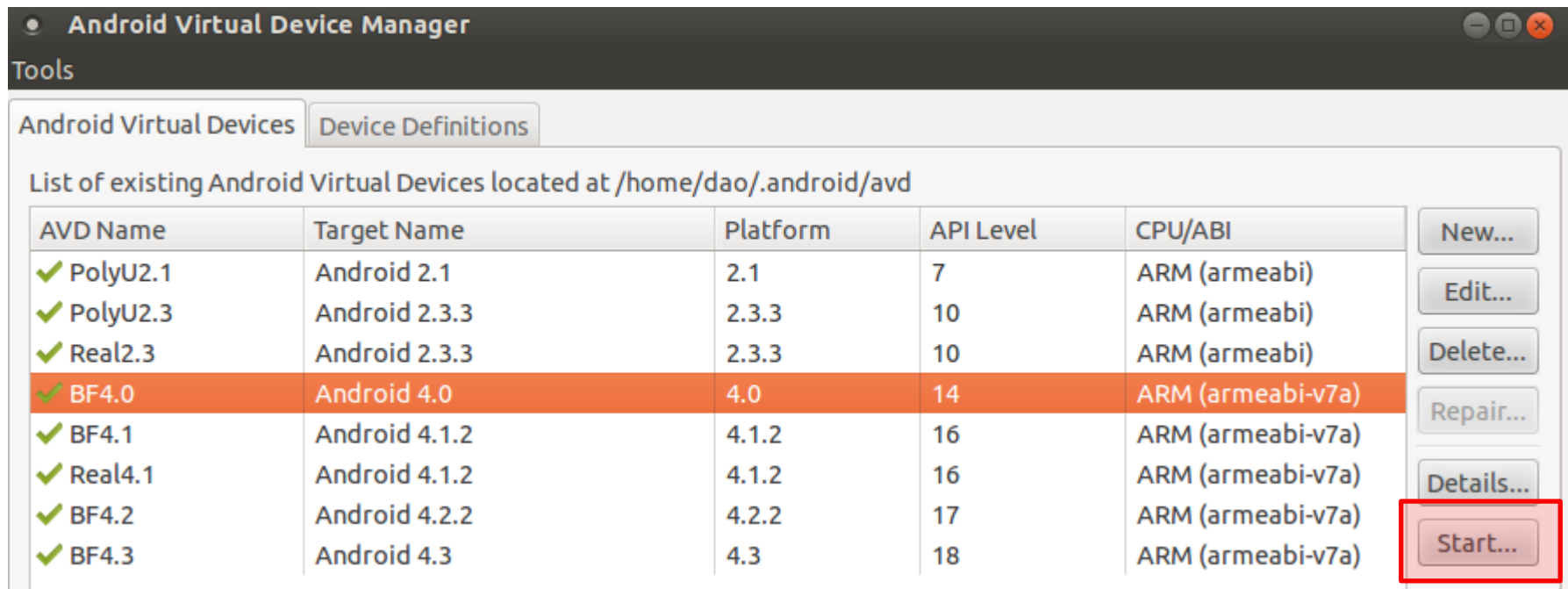
# AVD Manager (android avd)

- Create an AVD (Android Virtual Devices).
  - 4.0" Nexus S, Android 4.0, 300MB RAM, 50MB SD Card
- Windows: **AVD Manager.exe**



# Emulator (emulator)

- How to start a emulator?
  - In AVD Manager, select an avd, then click the “start” button.
  - Maybe a little bit long, have to wait ...





# (Optional) Using Hardware Devices for Analysis

- <http://developer.android.com/tools/device.html#setting-up>
  - Enable **USB debugging** on your device;
  - Set up your system to detect your device.
    - <http://developer.android.com/tools/extras/oem-usb.html#WinXp>
- Allow installation of apps from unknown sources
  - In your phone: Setting → Security → Select it.

# Android Debug Bridge (adb)

- android-sdk-windows\platform-tools\adb.exe
  - Use **command line** to run it, just type **adb** under this **directory**.
- List the current devices.

```
Y:\Win32\android-sdk-windows\platform-tools>adb devices
List of devices attached
emulator-5554  device  (other possible statuses are offline or bootloader)
```

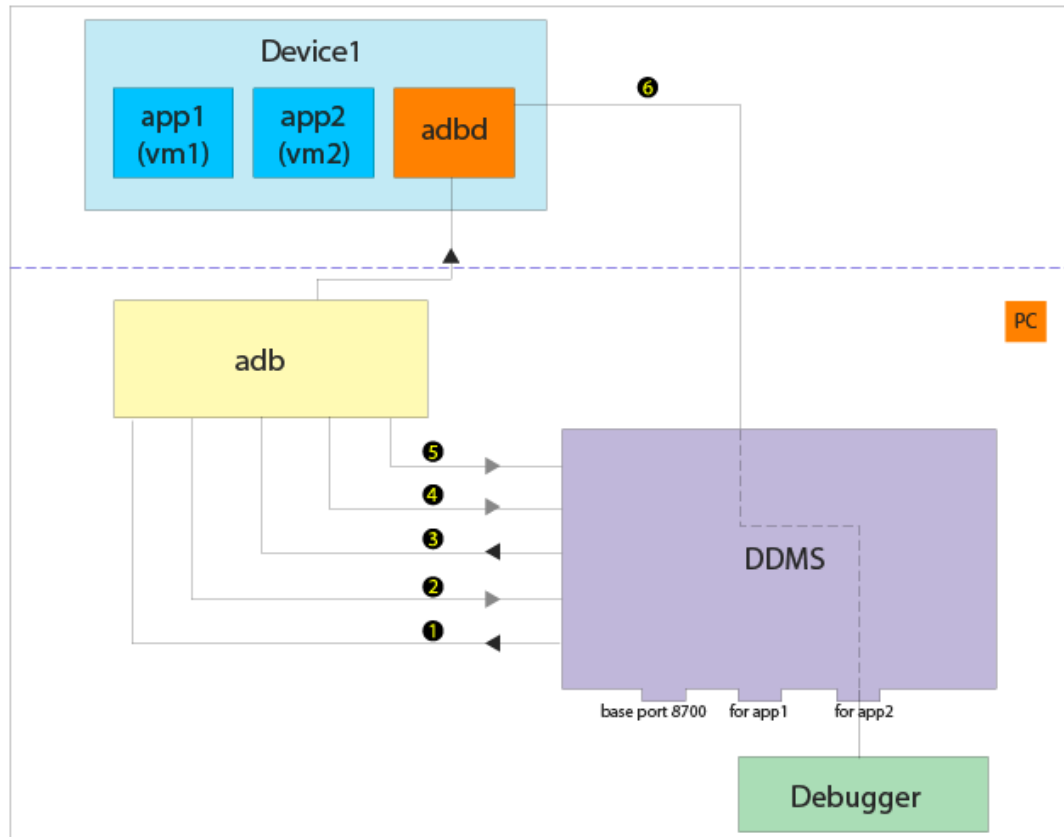
- Install an Android app (in PC) to emulator.

```
Y:\Win32\android-sdk-windows\platform-tools>adb install C:\andTest\yourapp.apk
59 KB/s (1862419 bytes in 30.531s)
  pkg: /data/local/tmp/yourapp.apk
Success
```

Download app from: <http://goo.gl/zzcGt1>

# ADB architecture

- Other useful commands: (such as **adb shell**)
  - Type **adb help** to query.



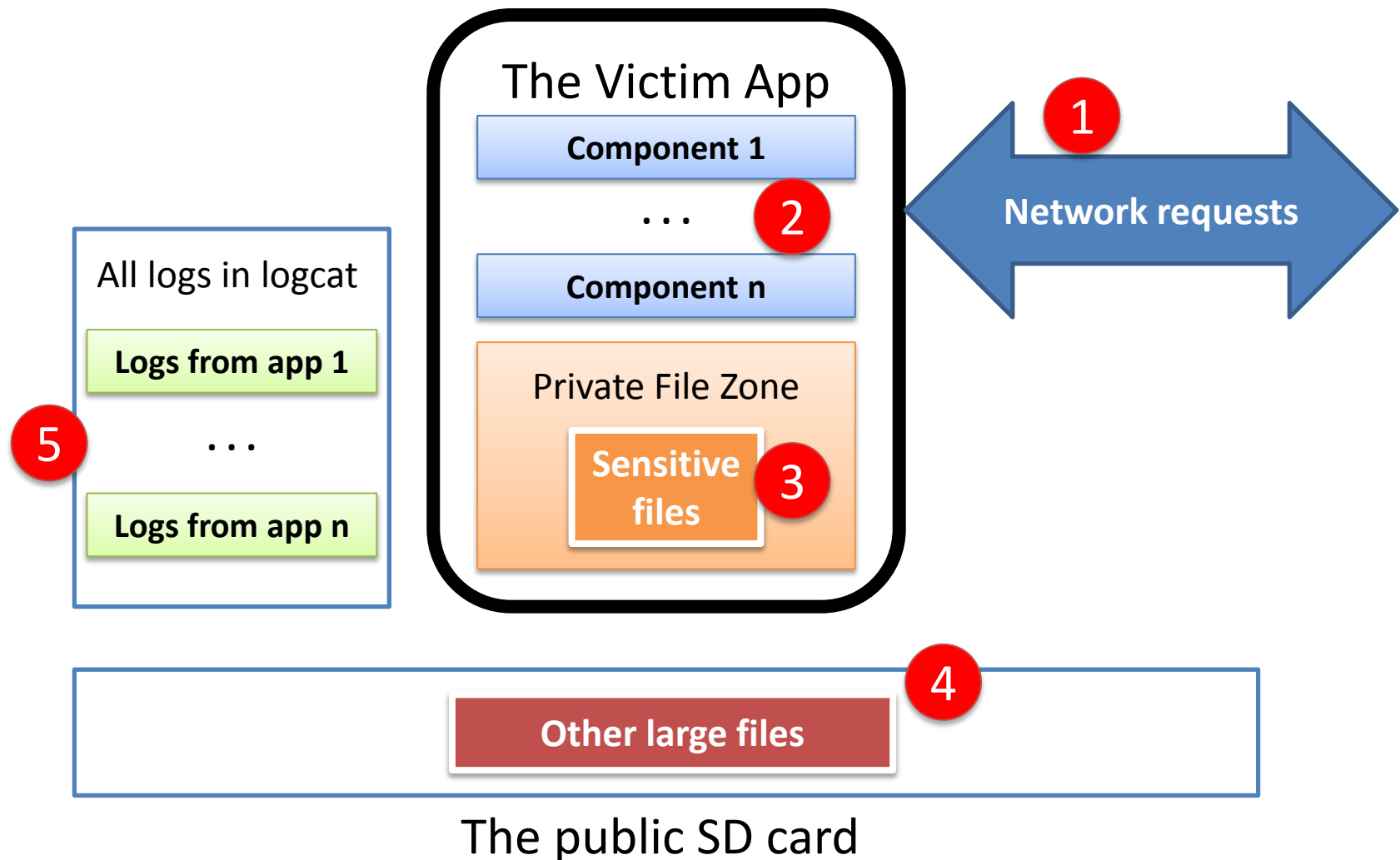
# Dalvik Debug Monitor Server (ddms)

- Provide UI control for some adb commands.
  - `android-sdk-windows\tools\ddms.bat`
- Follow the following practices:
  - Observe the listed processes.
    - Know the app package name we just installed.
  - Browse files in emulator using File Explorer.
  - **Pull files from emulator to PC.**
  - Capture the screen using Screen Capture button.
  - Monitor the log outputs using logcat command.
- One **important hint**:
  - Always remember to select the emulator or phone in the left side panel.

Understand Flaws in Android Apps

## **PART II: FLAWS IN ANDROID APPS**

# Overview of Potential Flaws

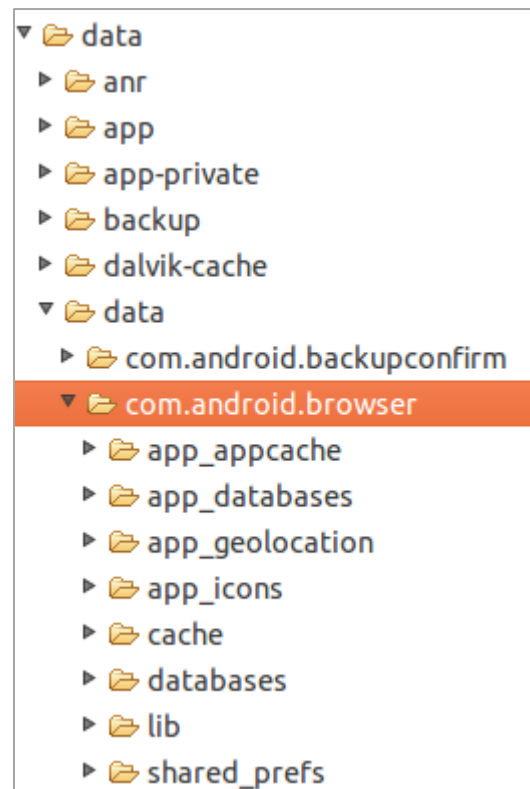


# Focus on insecure storage issues

- Insecure internal storage
  - Sometimes the assumption is that phones are rooted.
  - Sometime the file permissions are mis-configured.
- SD Card issue
  - Save cleartext-sensitive info to the public SD Card.
- Logcat issue
  - Output sensitive logs to the logcat.

# Insecure internal storage

- Android saves each app's internal files at:
  - /data/data/app-package





# Insecure internal storage: Skype

- Skype once mis-configured file permissions.

```
# ls -l /data/data/com.skype.merlin_mecha/files/shared.xml
-rw-rw-rw- app_152 app_152 56136 2011-04-13 00:07 shared.xml

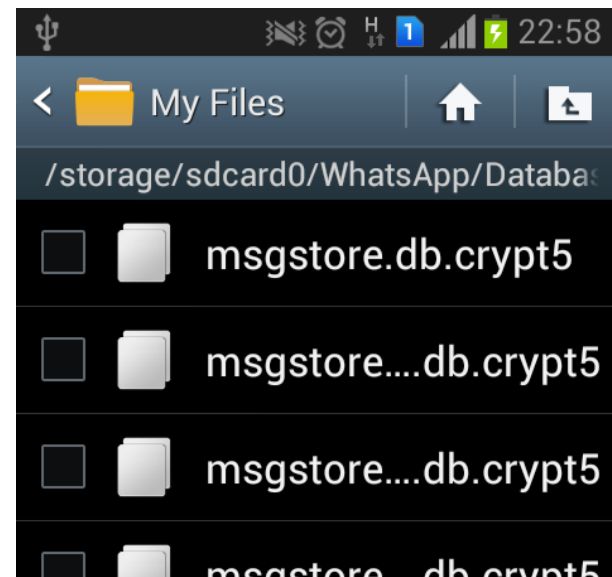
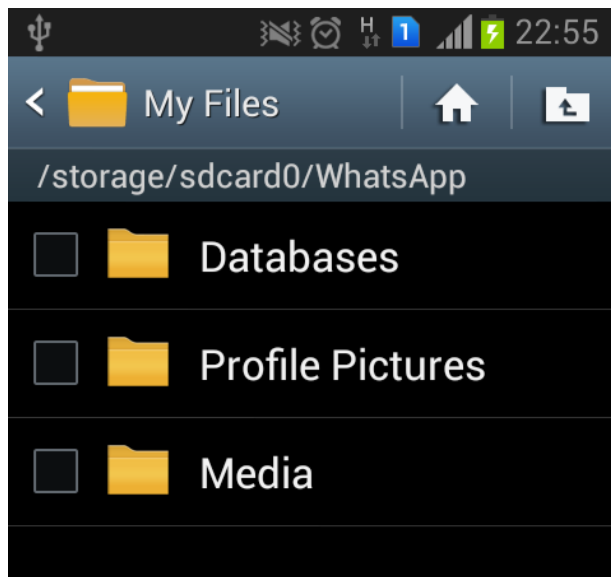
# grep Default /data/data/com.skype.merlin_mecha/files/shared.xml
<Default>jcaseap</Default>
```

Owner + Group + Other

```
# ls -l /data/data/com.skype.merlin_mecha/files/jcaseap
-rw-rw-rw- app_152 app_152 331776 2011-04-13 00:08 main.db
-rw-rw-rw- app_152 app_152 119528 2011-04-13 00:08 main.db-journal
-rw-rw-rw- app_152 app_152 40960 2011-04-11 14:05 keyval.db
-rw-rw-rw- app_152 app_152 3522 2011-04-12 23:39 config.xml
drwxrwxrwx app_152 app_152 2011-04-11 14:05 voicemail
-rw-rw-rw- app_152 app_152 0 2011-04-11 14:05 config.lck
-rw-rw-rw- app_152 app_152 61440 2011-04-13 00:08 bistats.db
drwxrwxrwx app_152 app_152 2011-04-12 21:49 chatsync
-rw-rw-rw- app_152 app_152 12824 2011-04-11 14:05 keyval.db-journal
-rw-rw-rw- app_152 app_152 33344 2011-04-13 00:08 bistats.db-journal
```

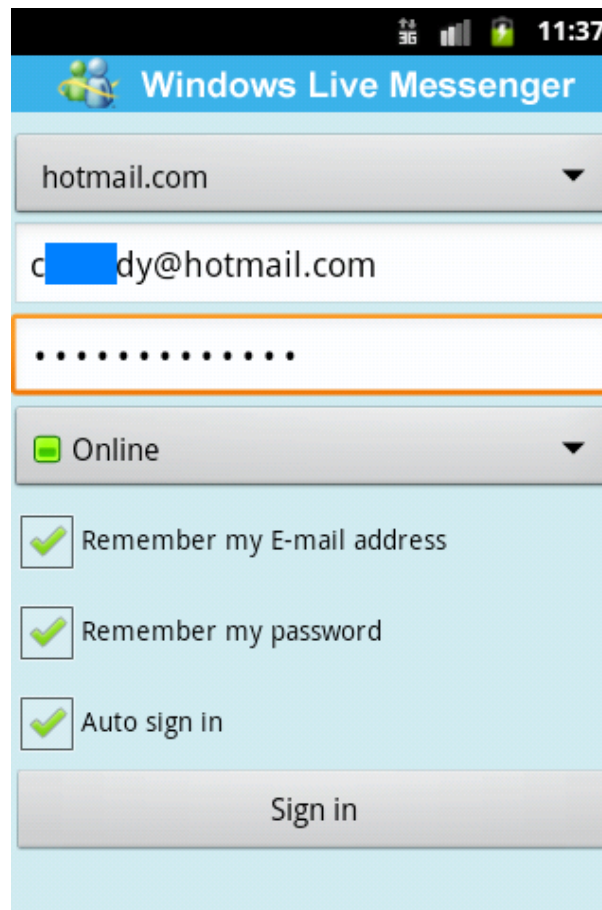
# SD Card issue

- Whatsapp saves some files in SD Card.
- If you have a phone,
  - You can browse them using a file manager.
    - <https://play.google.com/store/apps/details?id=org.opentints.filemanager>



# Logcat issue: MSN Password Leak

- Identify and test it using my own account.



The screenshot shows the Windows Live Messenger login screen on a mobile device. The status bar at the top indicates the time is 11:37. The app title "Windows Live Messenger" is displayed in a blue header. Below the header, there is a dropdown menu for the email provider, currently set to "hotmail.com". The email address field contains "c[redacted]dy@hotmail.com". The password field is highlighted with an orange border and contains ten dots. Below the password field is a dropdown menu for the account type, currently set to "Online". At the bottom, there are three checkboxes: "Remember my E-mail address", "Remember my password", and "Auto sign in", all of which are checked. A "Sign in" button is located at the very bottom.

# Logcat issue: MSN Password Leak

- Logcat in DDMS:

miyowa.android.microsoft	Proxy	CoreServiceOpenCommand sent = [9 -1 7 MSP3 1 0 c. dy@hotmail.
miyowa.android.microsoft	dalvikvm	GC_EXTERNAL_ALLOC freed 187K, 49% free 3156K/6087K, external 93
miyowa.android.microsoft	C2DM	Registration ID = null
miyowa.android.microsoft	C2DM	No Reg id, try to register
miyowa.android.microsoft	C2DM	Registration ID = null
miyowa.android.microsoft	C2DM	Sender email wmlbywithyou@gmail.com

email

pwd

CoreServiceOpenCommand sent = [9 -1 7 MSP3 1 0 c. dy@hotmail.com  STATUS_CLASS 256 ]
GC_EXTERNAL_ALLOC freed 187K, 49% free 3156K/6087K, external 934K/1530K, paused 54ms
Registration ID = null
No Reg id, try to register
Registration ID = null
Sender email wmlbywithyou@gmail.com

Practice your skills

## **PART III: EXERCISES**

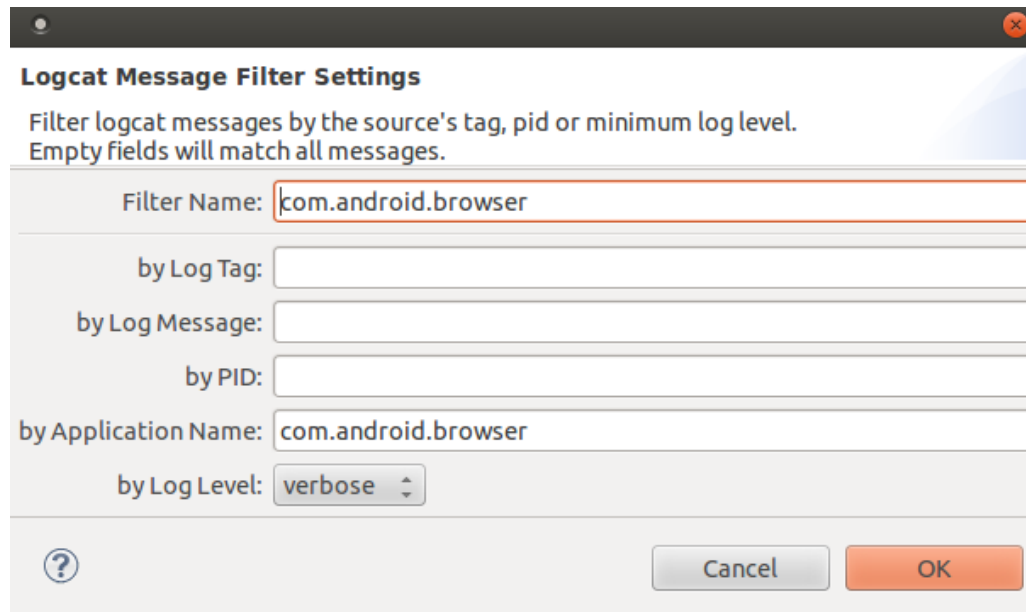
# Exercises

- In general,
  - Your answers should be supported by your screenshots.
  - I also assume you will never take the same screenshot.
  - Questions are simple, but you need to do them by yourselves.

Please hand in a hard copy of all exercise answers!

# Exercise #1

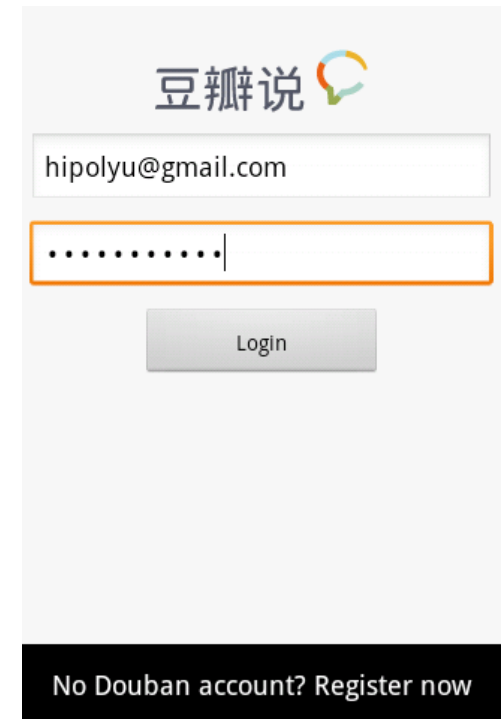
- **Set a logcat filter and give a screenshot of logcat outputs from the default Android browser. (5 marks)**
  - Hint: the filter is like this:



# Exercise #2

- In an app called Douban Shuo (<http://goo.gl/zzcGt1>), **where does it save an user's password to? Encrypted or not? Provide screenshots to support your answers.** (10 marks)
  - Hint: Under its *shared\_prefs* directory in internal storage.

<http://www.douban.com/>  
User:hipolyu@gmail.com  
Pwd: android2014

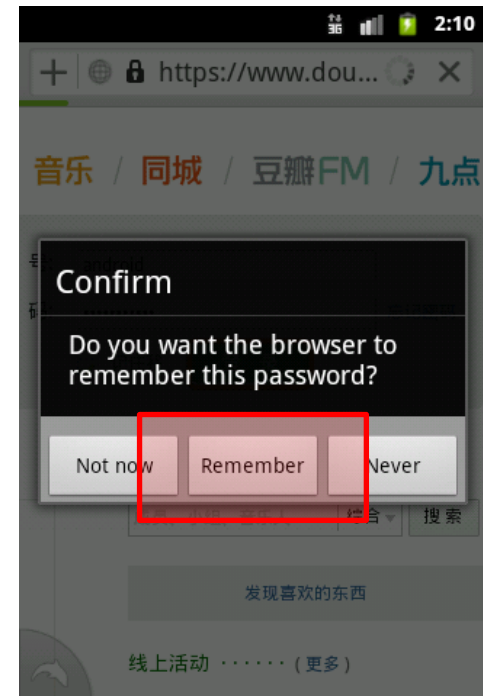




# Exercise #3

- In Android 4.0's default browser, suppose that an user chooses to remember his or her password.
  - Does the browser save the password in an encrypted form? Provide screenshots to support your answers. (10 marks)
  - Hint: the file name is **webview.db**.
  - Open it with *sqlite3* command in the *adb shell*. (then issue *.dump*)
    - <http://developer.android.com/tools/help/adb.html#sqlite>

<http://www.douban.com/>  
User:hipolyu@gmail.com  
Pwd: android2014



# Exercise #4

- An app called Xiao Xi Su Di (消息速递) saves users' messages in SD card. Suppose you have its SD card directory (<http://goo.gl/q3Zssw>), **please determine which file does it save messages to? Encrypted or not. (5 marks)**



Hint: use SQLite Database browser (<http://goo.gl/kpvPI>) to browse its database files.

# Questions?