Making WiGLE Data more Awesome

- What is WiGLE?
  - Patrick already told you (it's a wifi AP war driving site)
- How are we gonna do this?
  - Creating a fake network of APs and adding the data to WiGLE's db
    - While the network is fake, the individual 'APs' did exist at the time each one was sampled, therefore we are not simply adding false data to the db per se...

Fake AP Awesomeness!

- I will explain how to turn your device into an AP
  - This will be targeted towards devices like the Nexus 7 (2012), which do not have this feature enabled
- For many devices, you can do this easily:
  - *Settings → Wireless & Networks → more... → USB tethering & portable wifi hotspot*
- If you don't have this option, I'll tell you how to unlock, root, and install a super awesome custom version of Android.

B19 – Before the Trolling

Fake AP Awesomeness!

- No AP option on your phone? No Problem!!
- **Step 1**: Unlock bootloader
  - Make sure adb sees your device
    - *adb devices*
  - *adb reboot bootloader*
    - Reboots in fastboot mode
  - Make sure fastboot sees your device
    - *fastboot devices*
  - *fastboot oem unlock*
    - Select 'yes' from the phone (using power button)
    - This method will erase all your phat shizz on the device

Fake AP Awesomeness!

- I am having permissions issues according to adb when the device is in fastboot mode
  - Using linux eh? No worries, plenty of information online about these issues
  - Your trusty TA was too lazy to install the Android SDK on linux, so he used Windows....

Shameless Plug Awesomeness!

- Why does our trusty TA do stuff in Windows?
  - He likes to build awesome stuff like this:

  - This stuff needs Windows (also too lazy to reboot to linux)

Fake AP Awesomeness!

- **Step 2**: install custom recovery image
- Install recovery image
  - You wanna overwrite the default one
    - Download a **ClockworkMod** recovery image
  - Boot device into fastboot mode
    - *adb reboot bootloader*
  - *fastboot flash recovery <your_recovery_image>.img*
    - Make sure you download the recovery image to the same folder as fastboot is stored, or make sure the download folder is in your PATH
  - At this point, your phone is at the fastboot screen...

Fake AP Awesomeness!

- Boot into recovery mode
  - Use the volume keys to select *Recovery Mode*
  - Hit power to confirm selection
  - If it worked you should see a screen that says ClockworkMod recovery
- Wahhhhhh, what if I don't?
  - Did you boot the phone normally, then reboot again?
    - Sometimes this overwrites the recovery image with the stock one

Quick Note

- At this point, if all you want to do is **root your phone...**
  - Select the restart option (reboot system now), when it asks if you want to root the device, select yes

cyanogenmod!!

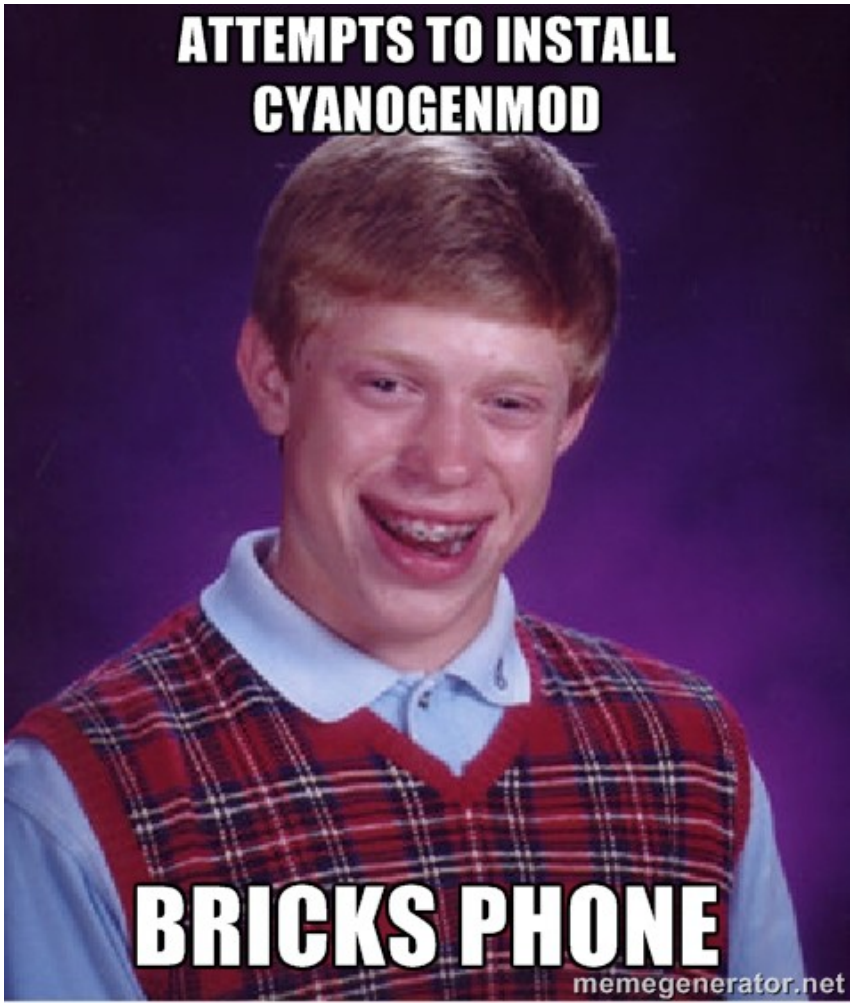
- **Step 3**: Let's install cyanogenmod!!
  - Custom Android (usually has AP support)
- Wipe data!
  - What?? Again??
    - Yes. It takes a couple seconds, it's cool yo
    - Select *wipe data/factory reset*
  - No!! I don't want to!!
    - Fine, then watch your cyanogenmod icon dude be mad at you (and you will be watching this for a long long time)

cyanogenmod!!

- Install cyanogenmod!!!!!!
  - Two methods
    - **Awesome** method: manually copy the downloaded cyanogenmod zip to your devices external storage
      - Or, simply download it directly onto your external from the device itself.
    - **Cool** method: sideload the cyanogenmod zip to the device directly in ClockworkMod
      - Laid back approach, but doesn't always work

cyanogenmod!!

- Install cyanogenmod!!!!!!
  - **Common to both methods:**
    - Download the latest cyanogenmod package (zip file)
      - Select the latest stable package which corresponds to your device
      - Hint: If one of our Nexus 7's, it's a *grouper* package



cyanogenmod!!

- Install cyanogenmod!!!!!!
  - **Awesome** method**:**
    - Make sure to have the cyanogenmod package zip file on your device's external storage
      - Here, external storage can be anything on your device which does NOT get wiped during a factory reset
      - Usually */sdcard* is good
    - You can do this by downloading on your computer and transferring to your device, or download directly on the device

cyanogenmod!!

- Install cyanogenmod!!!!!!
  - **Awesome** method**:**
    - What if my device has no external storage?
      - From within ClockworkMod, mount another partition:
        - *mounts and storage*
        - Mount something, such as */data*
        - Note: this requires adb to see your device!
    - Fortunately, most devices have some sort of external storage

cyanogenmod!!

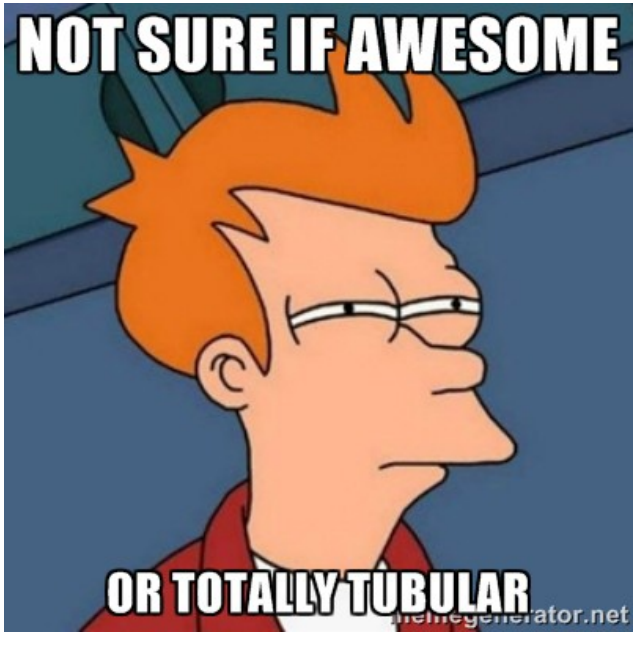
- Install cyanogenmod!!!!!!
  - **Awesome** method**:**
    - From ClockworkMod:
      - Wipe data!
        - What?? Again??
          - Yes. It takes a couple seconds, it's cool yo
      - Select *wipe data/factory reset*
        - No!! I don't want to!!
          - Fine, then watch your cyanogenmod icon dude be mad at you (and you will be watching this for a long long time)

cyanogenmod!!

- Install cyanogenmod!!!!!!
  - **Awesome** method**:**
    - From ClockworkMod:
      - Select *install zip*
      - Select *install zip from /sdcard*
        - Note: other paths besides */sdcard* may show up. Pick the one that corresponds to where you stored the cyanogenmod zip file.
      - Select the folders to get to the folder where you stored your cyanogenmod zip file
        - Usually /sdcard/0/....

cyanogenmod!!

- Install cyanogenmod!!!!!!
  - **Awesome** method**:**
    - From ClockworkMod:
      - Once the zip installation is complete....
        - Select *reboot system now*
        - Watch the awesomeness!!



cyanogenmod!!

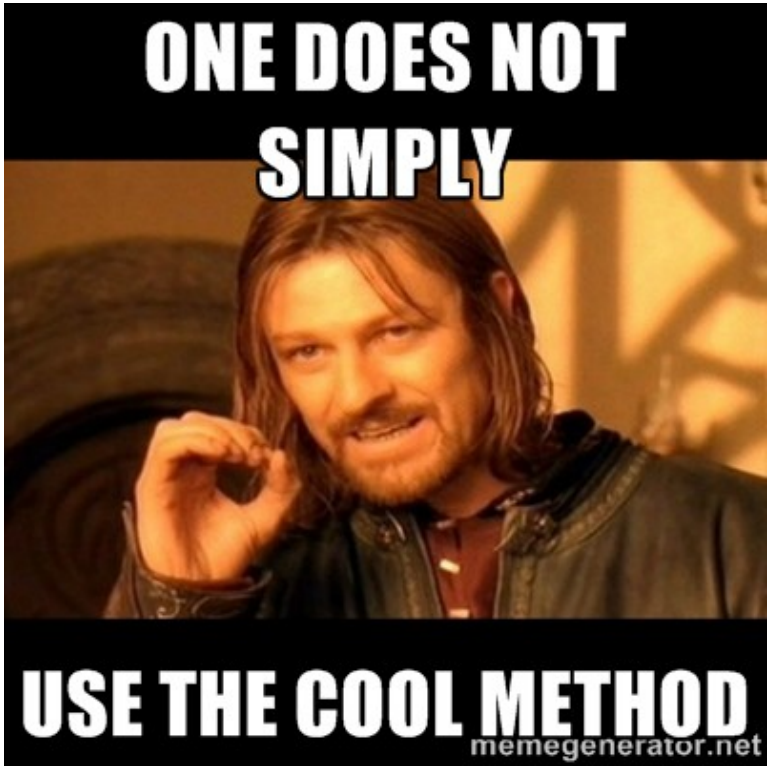
- Install cyanogenmod!!!!!!
  - **Cool** method**:**
    - Make sure you have the cyanogenmod zip file downloaded onto the computer
      - Put it in the same folder as your adb, fastboot executables (or make sure your download folder is in your PATH)

cyanogenmod!!

- Install cyanogenmod!!!!!!
  - **Cool** method**:**
    - From ClockworkMod:
      - Select *install zip*
      - Select *install zip from sideload*
    - From your computer:
      - *adb sideload <name_of_cyanogenmod_zip>*

cyanogenmod!!

- Install cyanogenmod!!!!!!
  - **Cool** method**:**
    - NOTE: If adb is not seeing your device, then use the **awesome** method instead

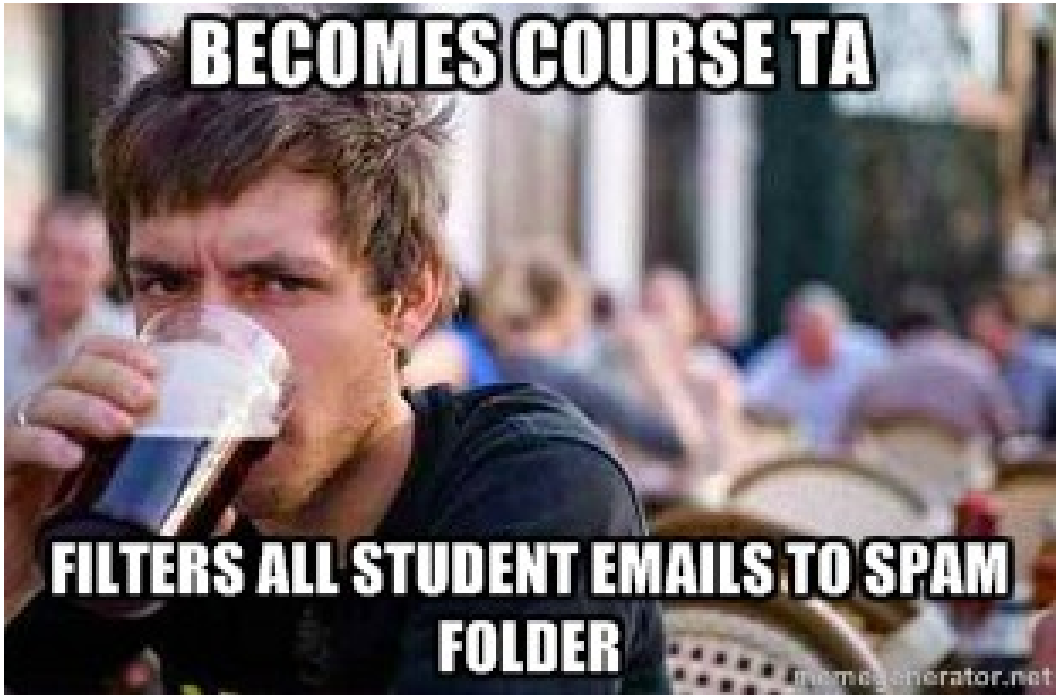


Fake AP Awesomeness!

- Depending on your specific cyanogenmod package (both version and target device), you may now be able to create an AP!
  - *Settings → Wireless & Networks → more... → USB tethering & portable wifi hotspot*
- What if only *USB tethering* shows up?
  - Nexus 7 user eh? No worries, these slides are written for you!

Fake AP Awesomeness!

- Your trusty TA stole some code from stackoverflow and used it to write his own soft AP app
  - Email the trusty TA for the app if you need it



Fake Networks of APs!

- How do we create a fake network of Aps?
  - Assuming you are war driving (WiGLE):
    - Use the same device, place it in multiple places, and at each place, reboot the device
      - Starting the AP after a fresh boot will cause the underlying API to generate a new random mac (BSSID) for the AP
        - The BSSID will be of the form: 02:1A:11:XX:XX:XX
          - This is standard behavior for Android devices when in AP mode.
        - WiGLE groups APs by BSSID, thus, each time you boot the device, it will appear to WiGLE as a separate AP (different BSSID, but with the same SSID)

B19 – After the Trolling