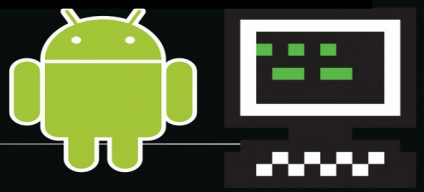
Android Security Auditing

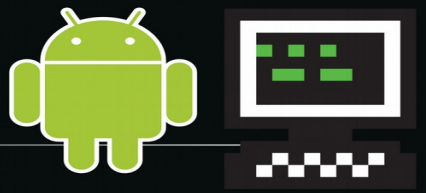
Investigating unauthorized screenshots of my activity

by Michael Altfield
https://www.michaelaltfield.net



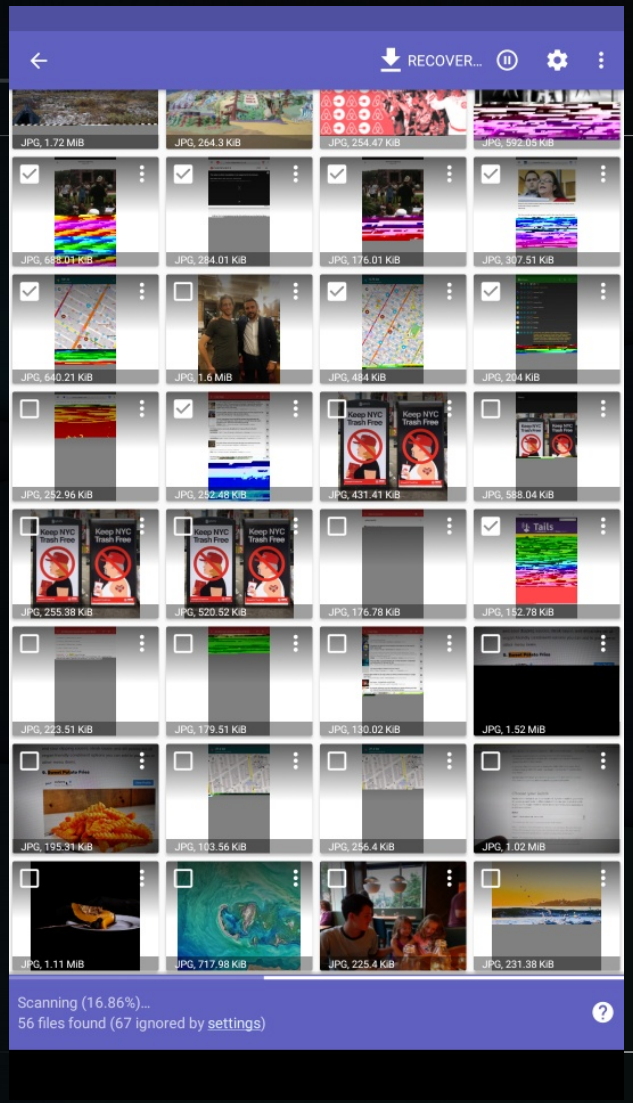
Context

- IamA Power User
- Nexus 5X (bullhead)
- ROM = Lineage OS 15.1 (8.1.0 Oreo)
- No Gapps
- Rooted
- IANA Android Dev



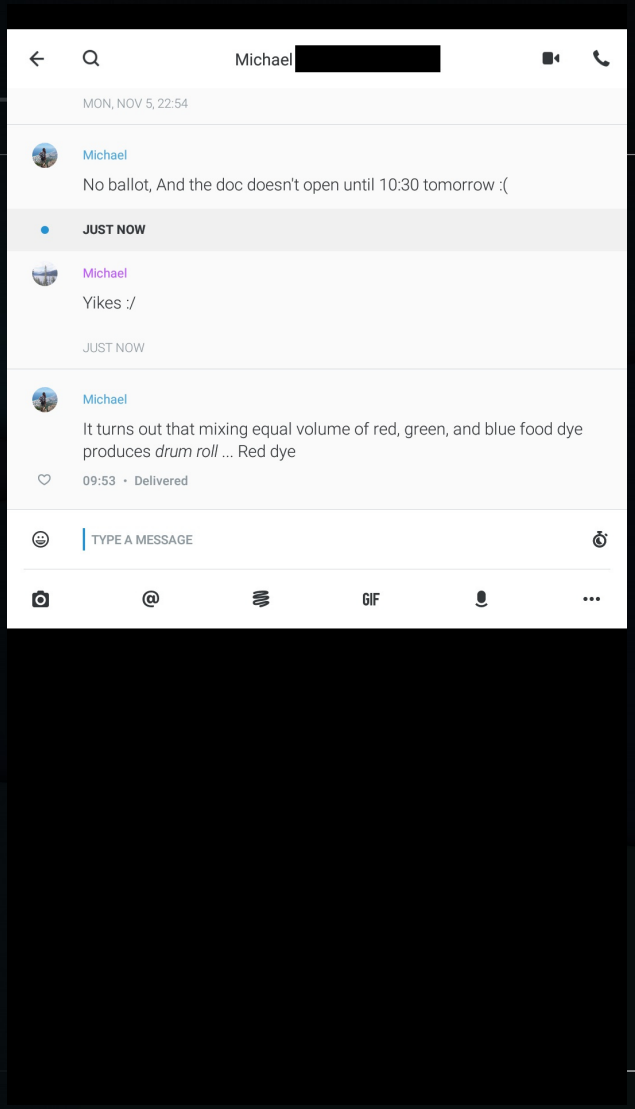
Discovery

DiskDigger
(Actual Image Files)



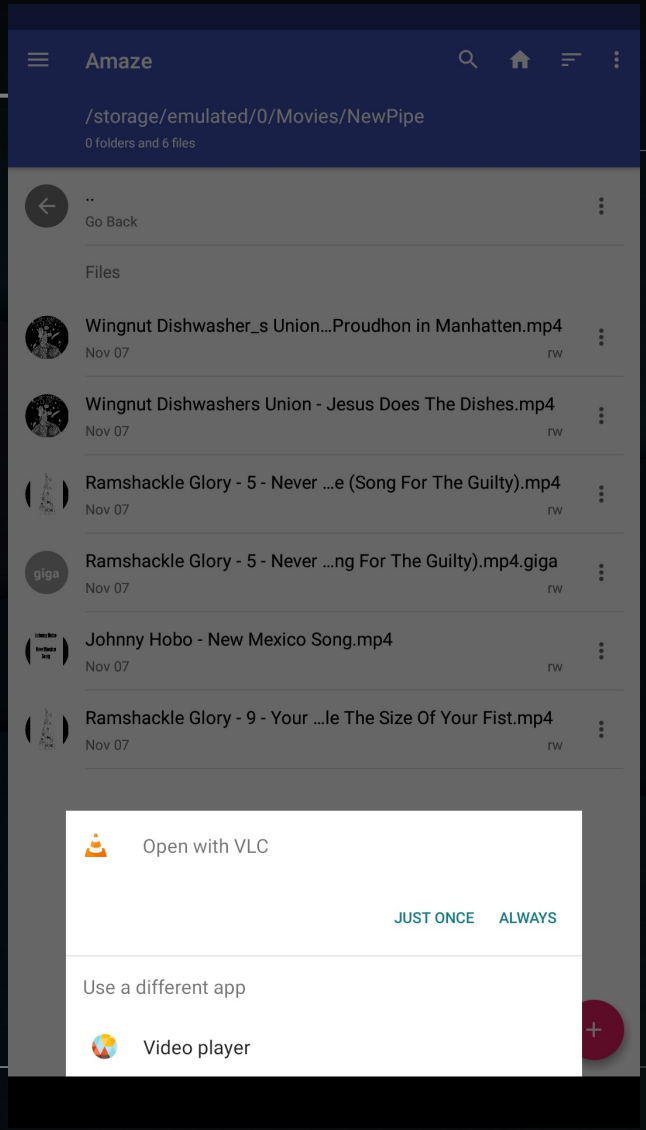
Discovery

Encrypted Conversations



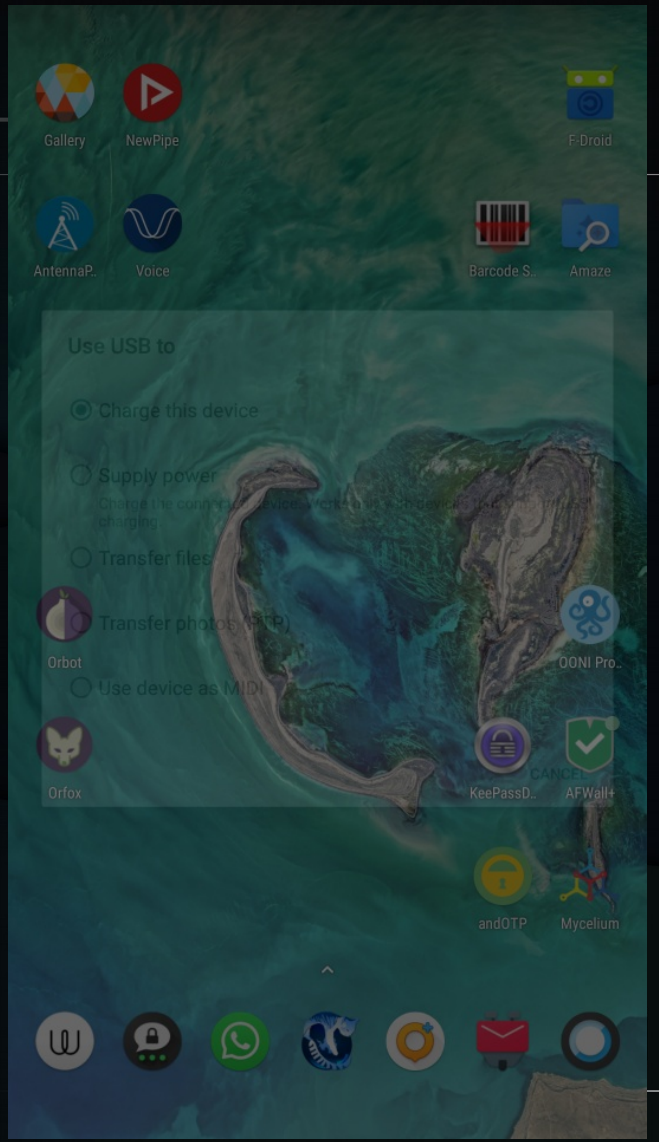
Discovery

Media Consumption



Discovery

Seemingly Useless

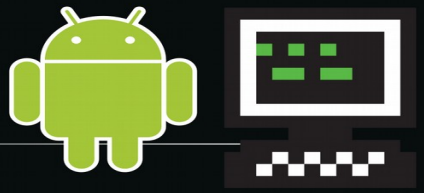


Discovery

Many Corrupt

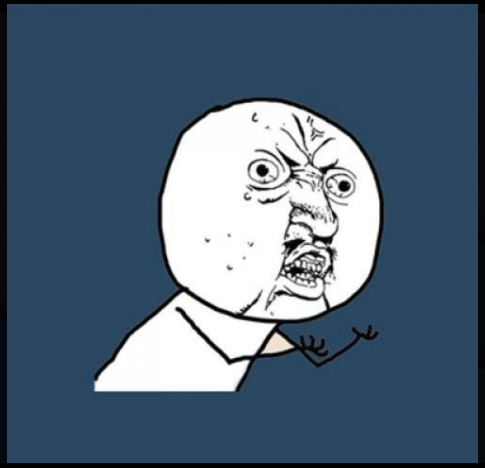
Approach #1: SELinux

- Since 2013, 4.3 (Jelly Bean) [1][2]
- Irony



Approach #1: SELinux (cont)

Google + /sepolicy



No `auditctl`

Intentional?

9.7. Security Features

...

[C-0-3] MUST NOT make SELinux or any other security features implemented below the Android framework configurable to the user or app developer.

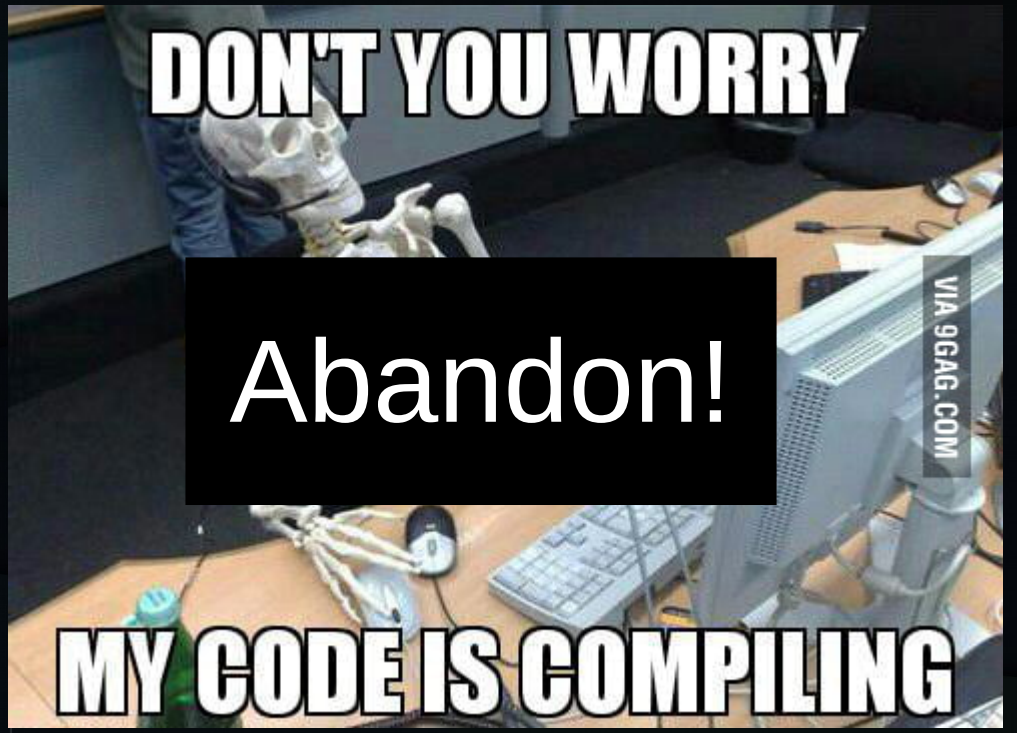
Source: Android 9 Compatibility Definition

Approach #1: SELinux (cont)

Hacking /sepolicy

Sepolicy-inject [1][2][3][4]

- >2 years old
- 100G
- compile errors galore



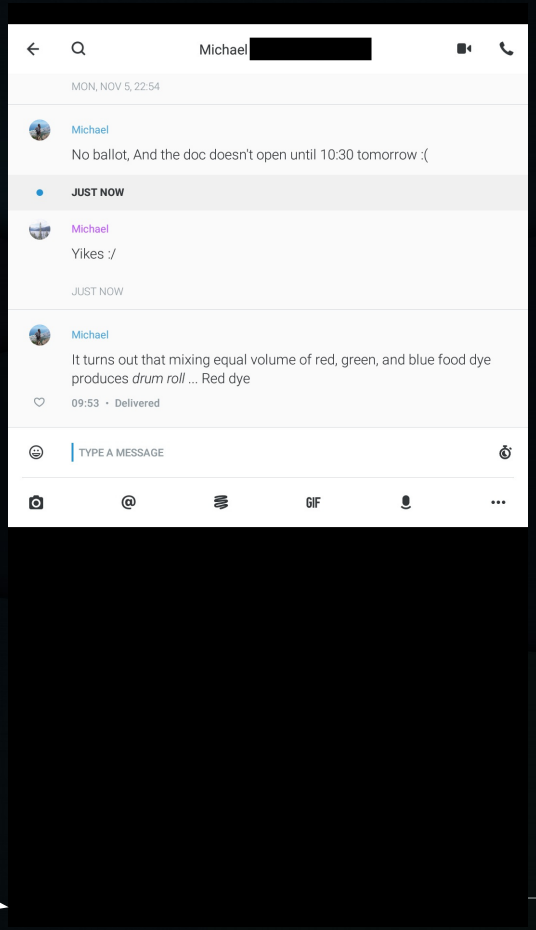
Approach #2: Files & Metadata

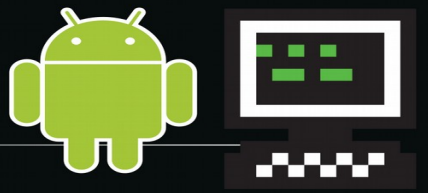
Top bar

Blacked-out

Keyboard area

Bottom bar

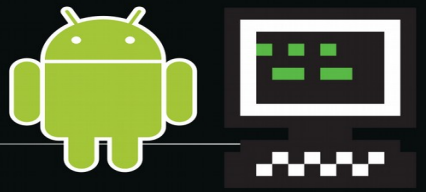




Approach #2: Files & Metadata

- JPG (not PNG)
- exif

```
michael@amy:/tmp$ exiftool 8064090112.jpg
…
Profile Copyright: Google Inc. 2016
```

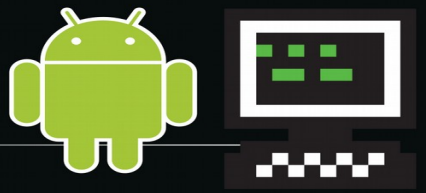


Approach #2: Files & Metadata

```
bullhead:/ $ find / -name *.jpg \
             1>/sdcard/findJpgs.txt
```

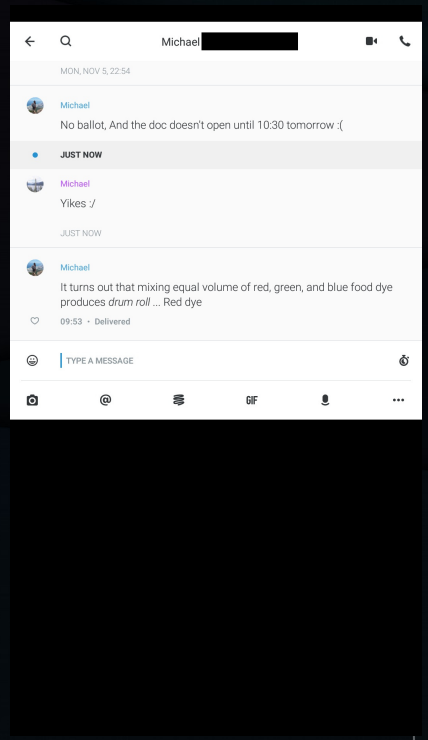
Approach #2: Files & Metadata

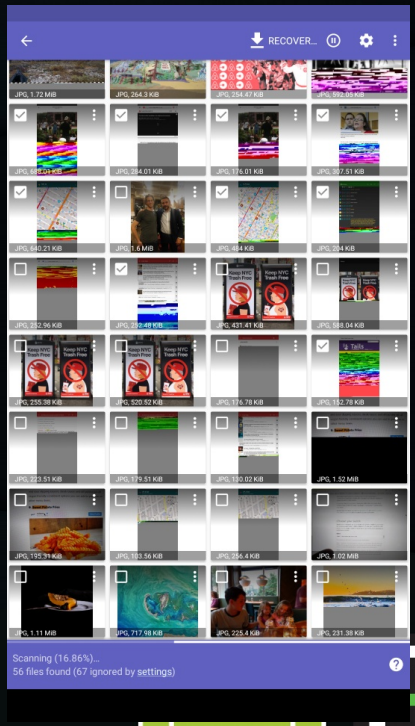
```
bullhead:/ # tail /sdcard/findJpgs.txt
...
/
data/system_ce/0/snapshots/3419_reduc
ed.jpg
/data/system_ce/0/snapshots/3419.jpg
bullhead:/ #
```

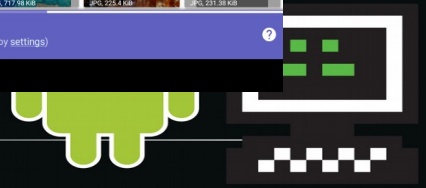


Approach #2: Files & Metadata

`/data/system_ce/0/snapshots`







Root Cause Identified!

Google “/data/system_ce/0/snapshots/”

TaskSnapshotPersister [1]

Recents Screen = Overview Screen

= Recent Task List = Recent Apps

aka “App Switcher” in iOS

Take-away

- Don’t be **too** paranoid [1][2][3][4]
- Google makes Android Sec Audit hard
- Devs: use FLAG_SECURE [1]