uc3m | Universidad Carlos III de Madrid

Grupo de investigación:
Computer Security Lab

Mobile Devices Security

Degree in Computer Engineering

2019

Introduction

Process of generic "rooting"

1. unlocking bootloader (Very dependent on the manufacturer)
2. Installation of custom recovery
3. Installation root Tool through recovery
4. Apps settings that can request elevated privileges

Basic nomenclature

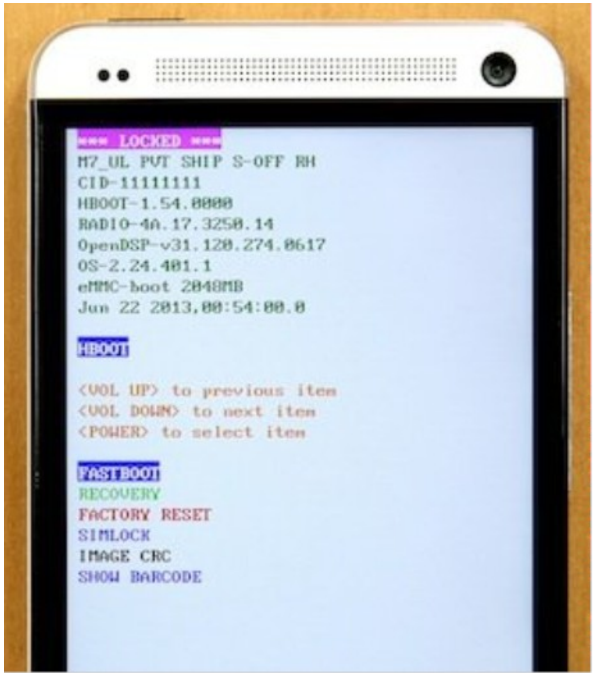
- Recovery (TWRP / CWM)
- partition
- root (SuperSU)
- (Hard | Soft) Brick
- kernel
- gpu
- Wipe
- Mount
- OTG
- nandroid Backup
- Development options (USB debug)
- boot Loop
- firmware | Radio
- Governor (CPU)
- Scheduler (I / O)
- fastboot
- adb
- Download Mode
- bootloader
- Unlock
- relock
- (Factory | Hard) reset
- Cache
- Flash
- debrand
- (Stock | Custom) ROM
- (Clean | Dirty) Flash

Partition structure

- / boot → start of the system (Kernel + ramdisk)
- / system → files from system + Applications preinstalled
- / Recovery → Tool with start own
- /data → Data of the user (Apps, SMS, configurations, etc..)
- /cache → Data temporary of apps
- /misc → State of the config from the dispositives HW between starts
- / EFS → IMEI, MAC.
- /sdcard → Internal Storage
- /sd-ext → internal storage (usually custom ROM)

bootloader

- The bootloader or boot loader is a program that is responsible for loading and executing the operating system after completing several tests automatic.
- Each manufacturer has his own.
- Factory is usually locked.
- For install SO's third must be unlocked first.
- Usually the warranty is lost to unlock bootloader.



```
*** LOCKED ***
M7_UL PVT SHIP S-OFF RH
CID-11111111
HBOOT-1.54.0000
RADIO-4A.17.3250.14
OpenDSP-v31.120.274.0617
OS-2.24.401.1
eMMC-boot 2048MB
Jun 22 2013,00:54:00.0

HBOOT

<VOL UP> to previous item
<VOL DOWN> to next item
<POWER> to select item

FASTBOOT
RECOVERY
FACTORY RESET
SIMLOCK
IMAGE CRC
SHOW BARCODE
```

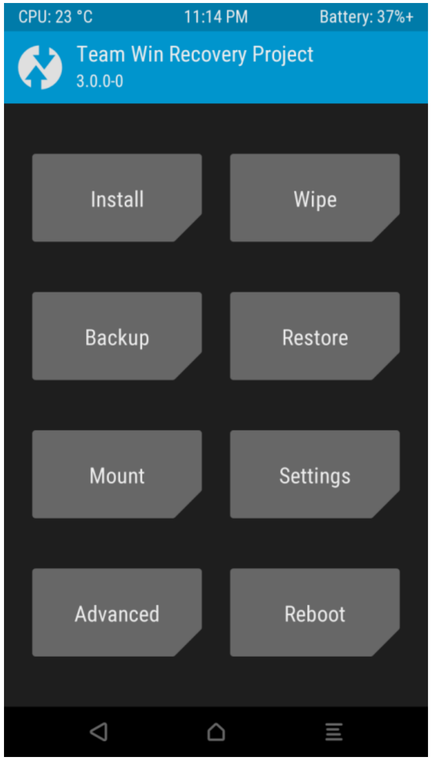
Recovery

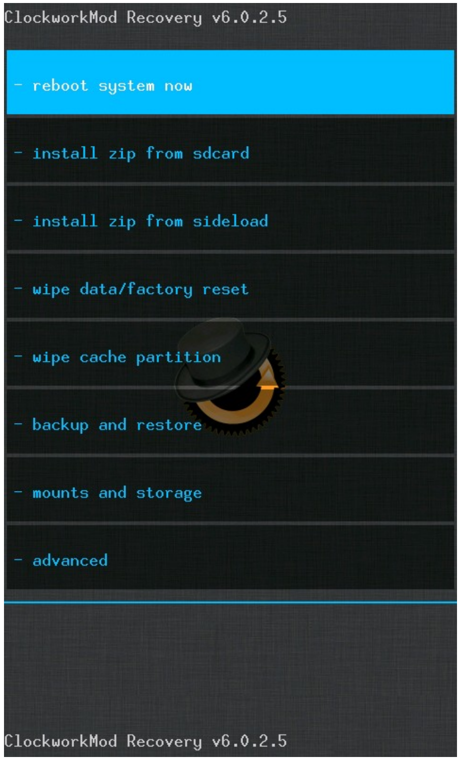
1. bootloader unlocked

- Autobootable partition independent of the operating system.
- bootable since bootloader or combination of buttons.
- Types:
  - Stock
  - Custom
- Tool:
  - Install packages /system (usually OTA's)
  - Hard reset
  - Other tools (usually only Custom)

Recovery

- The Custom Recovery most used:
  - TWRP → Team Win Recovery Project[1]
  - CWM → ClockWorkMod[2]




ClockworkMod Recovery v6.0.2.5
- reboot system now
- install zip from sdcard
- install zip from sideload
- wipe data/factory reset
- wipe cache partition
- backup and restore
- mounts and storage
- advanced
ClockworkMod Recovery v6.0.2.5

[1] https://twrp.me

[2] http://www.clockworkmod.com

root

1. bootloader unlocked
2. Recovery installed

- **Root** It is the user account that, by default, have access to all commands and files on a Linux operating system. Also called **Super user**.

- Default Android → No privileged access
- Installing SW (OTA) by recovery manufacturer

- Types
  - Hard-rooting (Flash binary "your")
  - Soft-rooting (Taking advantage of a "root exploit")

Root

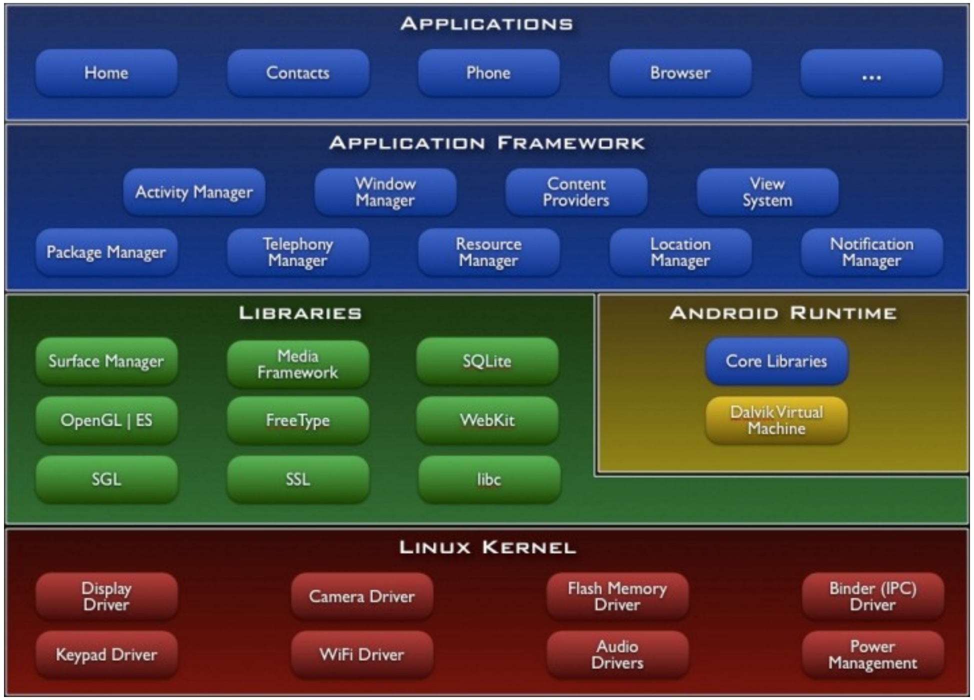
- Advantage
  - Total control parameters kernel
  - Total control applications, ability to uninstall apps preinstalled on /system
  - Modification of the characteristics of OS (Modules Xposed)

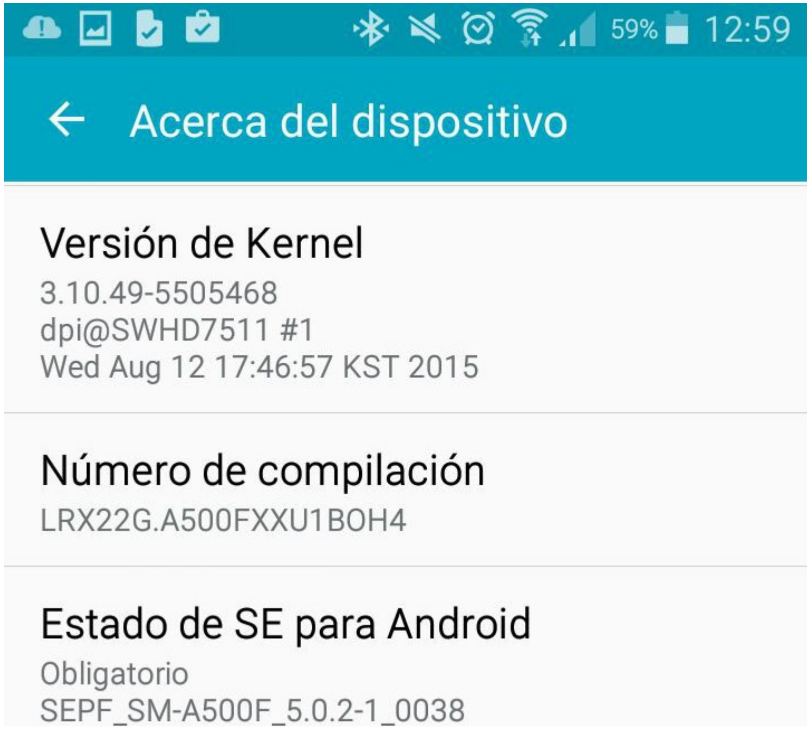
- Disadvantages
  - Possible loss of warranty by the manufacturer
  - delicate process: (Soft | Hard) Brick
  - the ability to update via OTA is lost
  - More vulnerable to malware

Kernel

1. bootloader unlocked
2. Recovery installed
3. root installed

- It is responsible for managing resources through system calls.





Acerca del dispositivo

Versión de Kernel

3.10.49-5505468
dpi@SWHD7511 #1
Wed Aug 12 17:46:57 KST 2015

Número de compilación

LRX22G.A500FXXU1BOH4

Estado de SE para Android

Obligatorio
SEPF_SM-A500F_5.0.2-1_0038

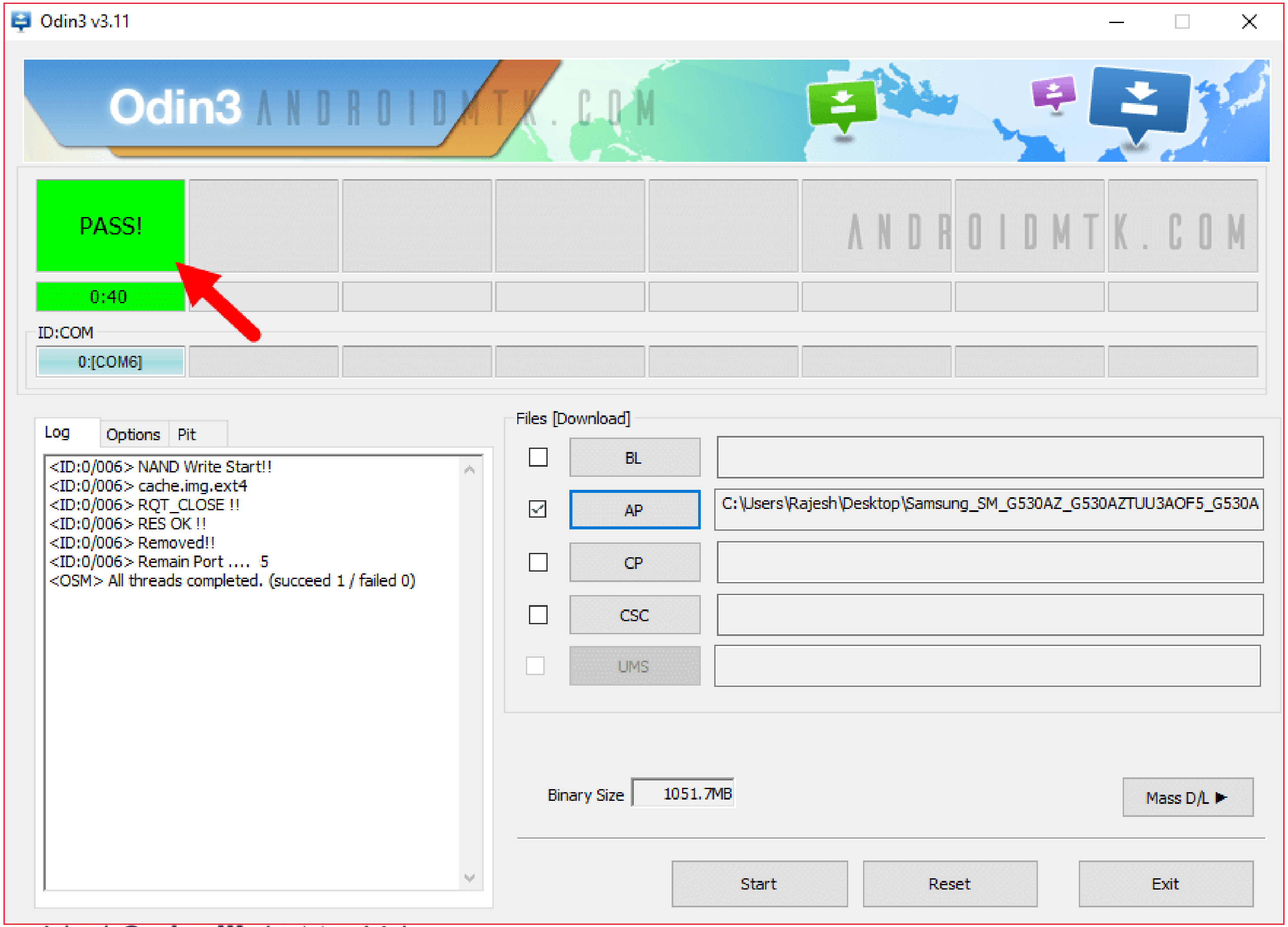
kernel

- basic parameters
  - CPU speed
  - Governor → Behavior CPU frequency
    - OnDemand: + Fluency | -Autonomy
    - Performance: Fluidity ++ | --Autonomy
    - powersave: --Fluidez | ++ Autonomy
    - Conservative(P + O): -Fluidez | + Autonomy
  - hotplug Driver → controlling use number CPU's
    - mpdecision: Default Driver Qualcomm → + Fluidity
    - msm_hotplug: Custom mpdecision from myflux → ++ Autonomy
    - Intelliplug: Custom hotplug Fluidity of faux123 → & Autonomy
  - Planner I / O

Tools

- Odin [Samsung]
- Ruus (Rom Upgrade Utilities) [HTC]
- MiFlash [Xiaomi]
- SP Flash Tool [Generic CPU's MTK]
- fastboot [Google | OnePlus| Sony]
- adb [OnePlus]

Odin



```
<ID:0/006> NAND Write Start!!
<ID:0/006> cache.img.ext4
<ID:0/006> RQT_CLOSE !!
<ID:0/006> RES OK !!
<ID:0/006> Removed!!
<ID:0/006> Remain Port ....  5
<OSM> All threads completed. (succeed 1 / failed 0)
```

□ BL

☑ AP C:\Users\Rajesh\Desktop\Samsung_SM_G530AZ_G530AZTUU3AOF5_G530A

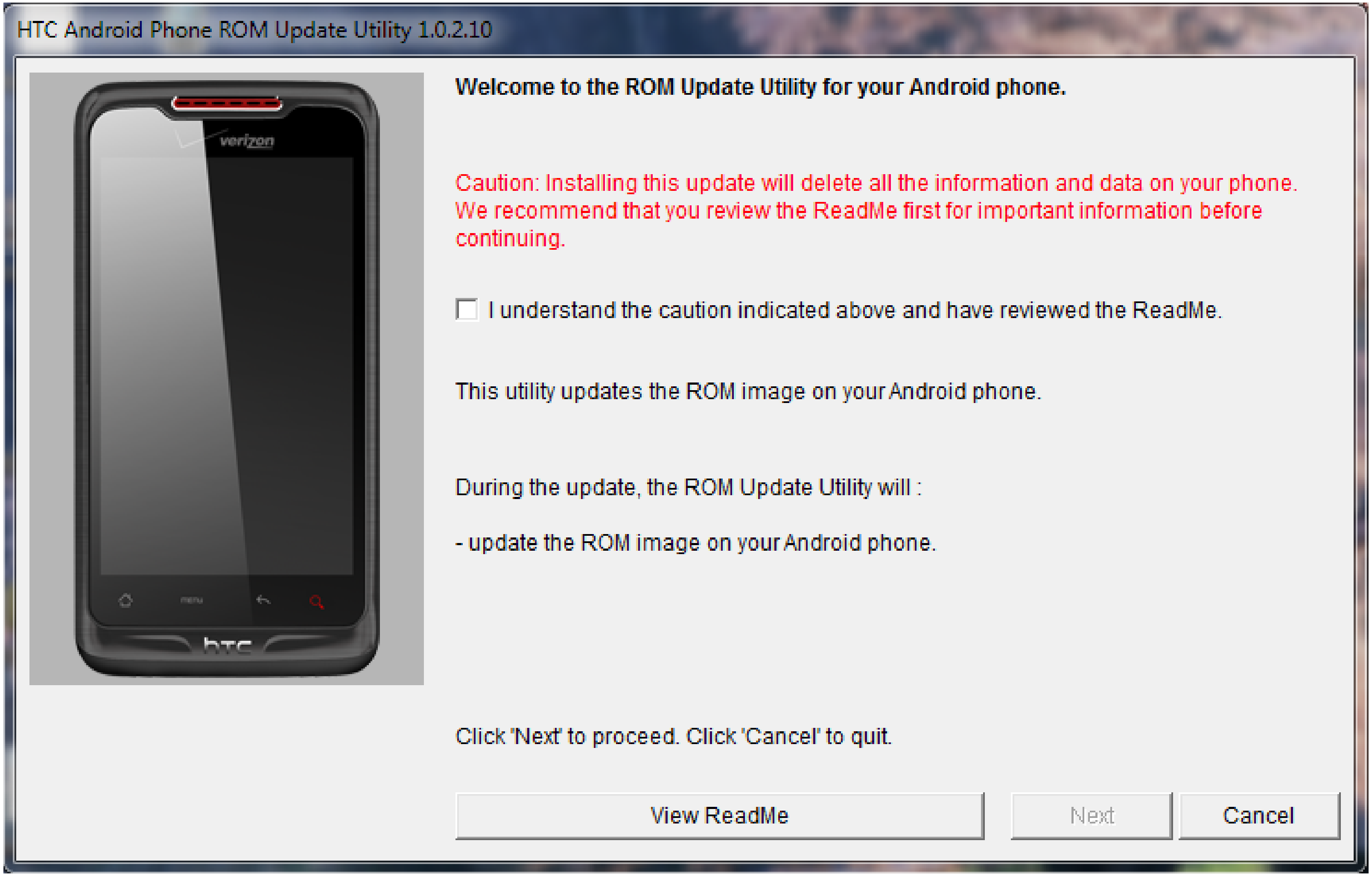
□ CP

□ CSC

□ UMS

Binary Size 1051.7MB

Ruus



HTC Android Phone ROM Update Utility 1.0.2.10

Welcome to the ROM Update Utility for your Android phone.

Caution: Installing this update will delete all the information and data on your phone. We recommend that you review the ReadMe first for important information before continuing.

□ I understand the caution indicated above and have reviewed the ReadMe.

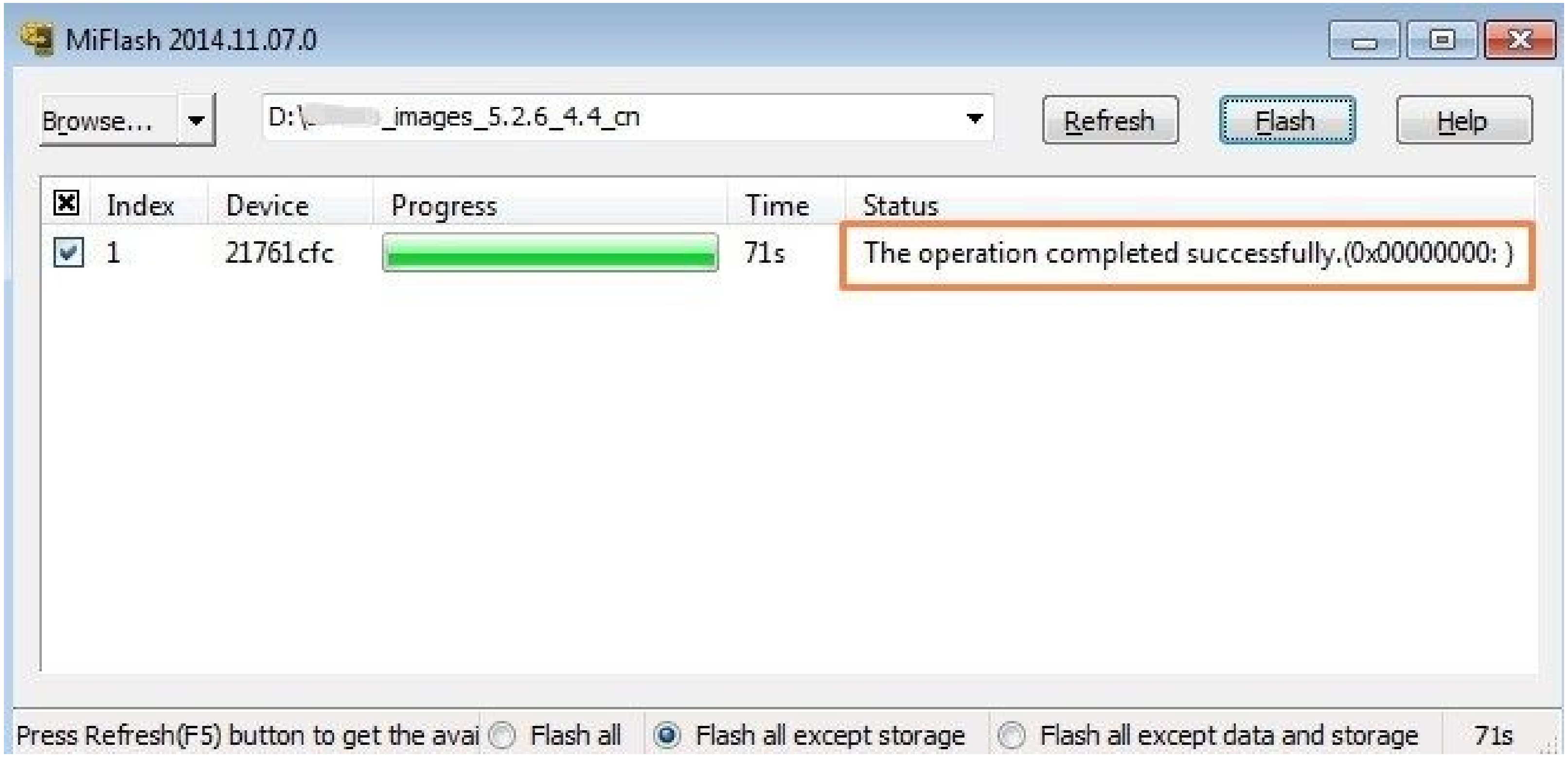
This utility updates the ROM image on your Android phone.

During the update, the ROM Update Utility will :

- update the ROM image on your Android phone.

Click 'Next' to proceed. Click 'Cancel' to quit.

MiFlash

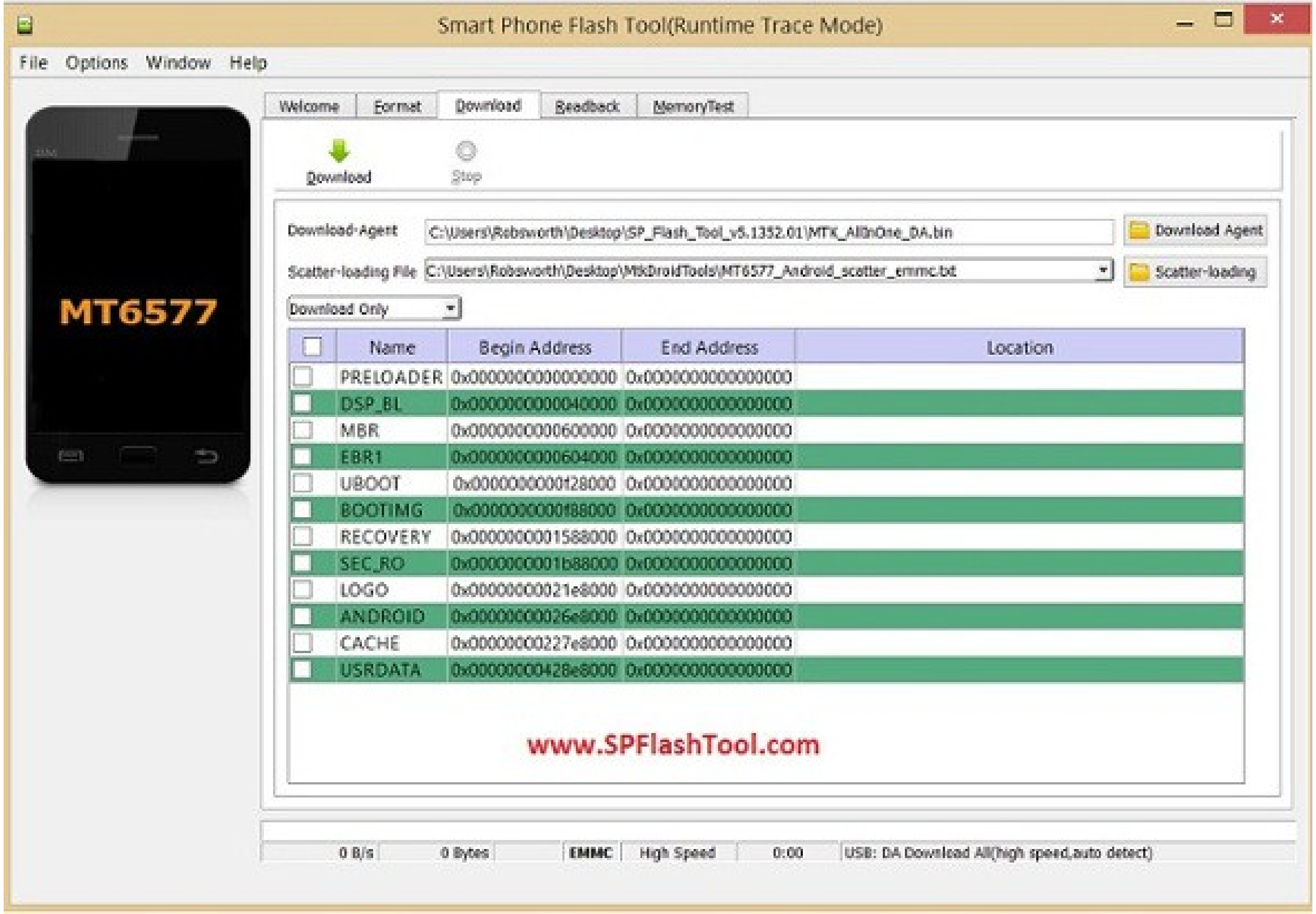


D:\[redacted]_images_5.2.6_4.4_cn

☒	Index	Device	Progress	Time	Status
☑	1	21761cfc	🟩	71s	The operation completed successfully.(0x00000000:)

Press Refresh(F5) button to get the avai ○ Flash all ● Flash all except storage ○ Flash all except data and storage 71s

SP Flash Tool



Smart Phone Flash Tool(Runtime Trace Mode)

Download-Agent: C:\Users\Robsworth\Desktop\SP_Flash_Tool_v5.1352.01\MTK_AllInOne_DA.bin

Scatter-loading File: C:\Users\Robsworth\Desktop\MtkDroidTools\MT6577_Android_scatter_emmc.txt

Download Only

□	Name	Begin Address	End Address	Location
□	PRELOADER	0x0000000000000000	0x0000000000000000	
□	DSP_BL	0x0000000000040000	0x0000000000000000	
□	MBR	0x0000000000600000	0x0000000000000000	
□	EBR1	0x0000000000604000	0x0000000000000000	
□	UBOOT	0x0000000000128000	0x0000000000000000	
□	BOOTIMG	0x0000000000188000	0x0000000000000000	
□	RECOVERY	0x0000000001588000	0x0000000000000000	
□	SEC_RO	0x0000000001b88000	0x0000000000000000	
□	LOGO	0x00000000021e8000	0x0000000000000000	
□	ANDROID	0x00000000026e8000	0x0000000000000000	
□	CACHE	0x00000000227e8000	0x0000000000000000	
□	USRDATA	0x00000000428e8000	0x0000000000000000	

www.SPFlashTool.com

0 B/s | 0 Bytes | EMMC | High Speed | 0:00 | USB: DA Download All(high speed,auto detect)

fastboot

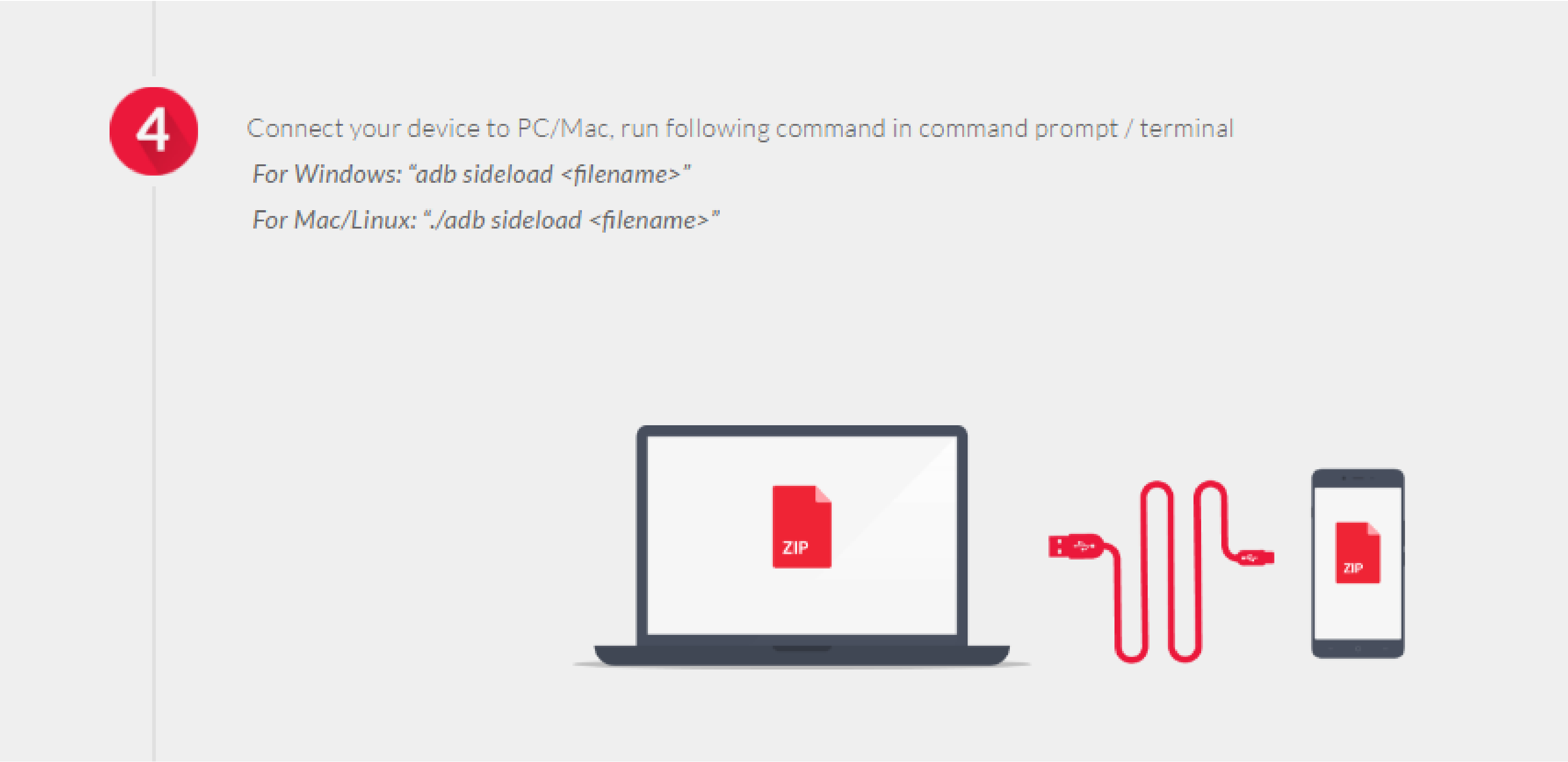
- Protocol of diagnosis included in SDK
- Function principal → Modify he system from files
- Needs to RESTARTING in mode bootloader

- [Sample] manufacturers what accept saying method:
  - Family Nexus
  - Sony XPeria
  - OnePlus

Example fastboot

```
@echo off
threw out #################################################
##########
threw out #######   Este Patch is Created by @sarathchakru   ########
echo # https://forums.oneplus.net/members/sarathchakru.200929/ #
threw out #################################################
##########
threw out .
threw out .
threw out # Este patch Should only be used for OnePlus ONE 64GB #
echo # Note: Este patch will erease whole data in your OPO 64GB #
threw out #############################
threw out # Model: OnePlus One 64GB #
threw out # bootloader: Unlocked      #
threw out #############################
threw out # Press any key if you want to continue otherways close Este window
#
pause
threw out .
threw out .
threw out # Connect EPO in fastboot mode #
threw out # your Device Id will be Appear despues de Este With fastboot mode #
threw out # If not, check your drivers and USB cable connection #
fastboot Devices
pause
threw out .
threw out .
threw out # Press any key to start Flashing #
pause
threw out .
threw out .

threw out # bootloader status #
fastboot oem device-info

threw out # Flashing Radio...#
fastboot flash aboot emmc_appsboot.mbn
fastboot flash LOGO logo.bin
fastboot flash modem NON-HLOS.bin
fastboot flash rpm rpm.mbn
fastboot SBL1 flash sbl1.mbn
fastboot flash DBI sdi.mbn
fastboot flash oppostanvbk static_nvbk.bin
fastboot flash tz tz.mbn

threw out # Flashing System Boot, Recovery, Cache and Userdata...
#
fastboot flash boot boot.img
fastboot flash recovery recovery.img
fastboot flash system system.img
fastboot flash cache cache.img
fastboot flash userdata userdata_64G.img

threw out # rebooting Phone... #
fastboot reboot

threw out .
threw out .
threw out #####################
threw out # Item is done now :) #
threw out # Happy fashing     #
threw out #####################
pause
```

adb



4

Connect your device to PC/Mac, run following command in command prompt / terminal

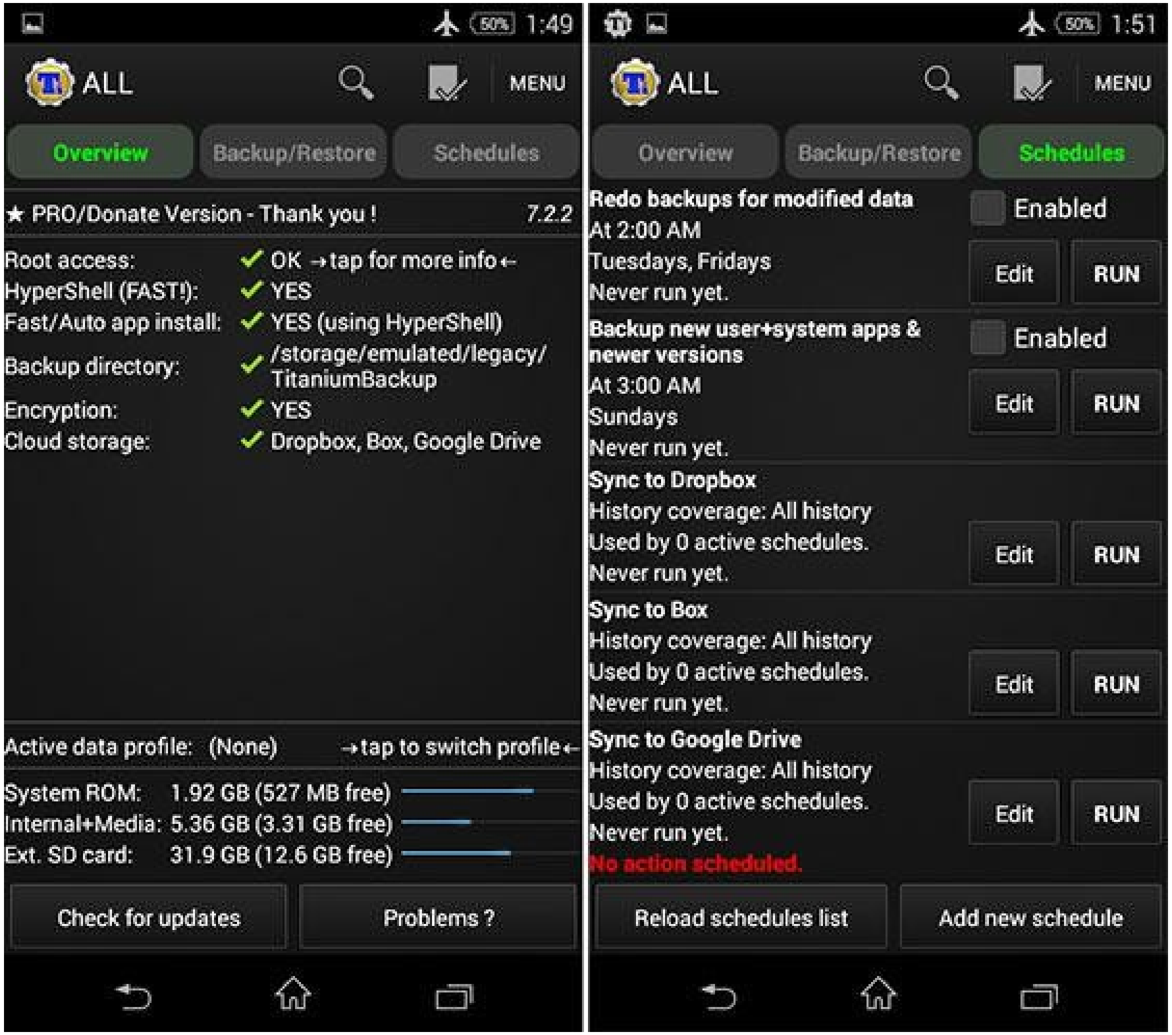
For Windows: "adb sideload <filename>"

For Mac/Linux: "./adb sideload <filename>"

Useful applications [ROOT]

- Titanium Backup
- Adaway
- WPS Connect
- It's File Explorer
- Xposed
- wakelock Detector

Titanium Backup



★ PRO/Donate Version - Thank you ! 7.2.2

Root access:	✓ OK →tap for more info←
HyperShell (FAST!):	✓ YES
Fast/Auto app install:	✓ YES (using HyperShell)
Backup directory:	✓ /storage/emulated/legacy/TitaniumBackup
Encryption:	✓ YES
Cloud storage:	✓ Dropbox, Box, Google Drive

Active data profile: (None) →tap to switch profile←

System ROM:	1.92 GB (527 MB free)
Internal+Media:	5.36 GB (3.31 GB free)
Ext. SD card:	31.9 GB (12.6 GB free)

Redo backups for modified data
At 2:00 AM
Tuesdays, Fridays
Never run yet.
□ Enabled

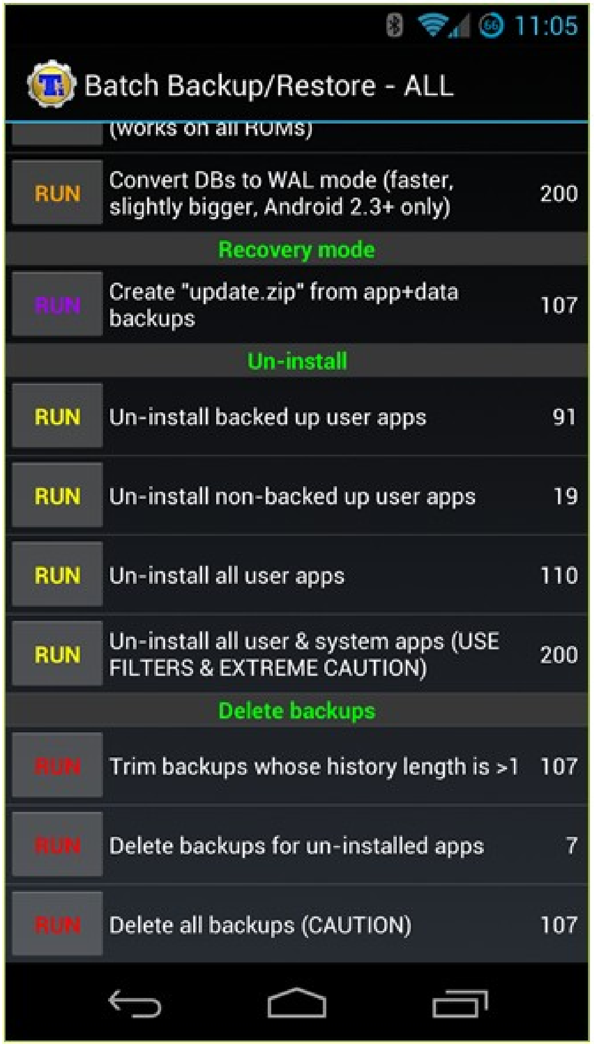
Backup new user+system apps & newer versions
At 3:00 AM
Sundays
Never run yet.
□ Enabled

Sync to Dropbox
History coverage: All history
Used by 0 active schedules.
Never run yet.

Sync to Box
History coverage: All history
Used by 0 active schedules.
Never run yet.

Sync to Google Drive
History coverage: All history
Used by 0 active schedules.
Never run yet.
No action scheduled.

Titanium Backup



11:05

Batch Backup/Restore - ALL

(works on all ROMs)

RUN	Convert DBs to WAL mode (faster, slightly bigger, Android 2.3+ only)	200

Recovery mode

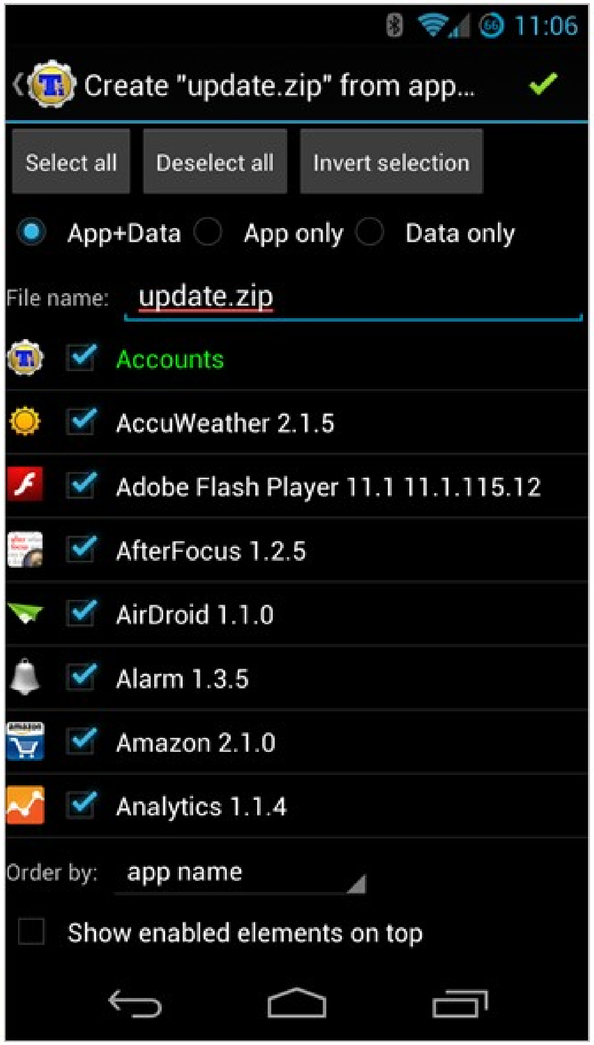
RUN	Create "update.zip" from app+data backups	107

Un-install

RUN	Un-install backed up user apps	91
RUN	Un-install non-backed up user apps	19
RUN	Un-install all user apps	110
RUN	Un-install all user & system apps (USE FILTERS & EXTREME CAUTION)	200

Delete backups

RUN	Trim backups whose history length is >1	107
RUN	Delete backups for un-installed apps	7
RUN	Delete all backups (CAUTION)	107



11:06

Create "update.zip" from app... ✓

Select all | Deselect all | Invert selection

● App+Data ○ App only ○ Data only

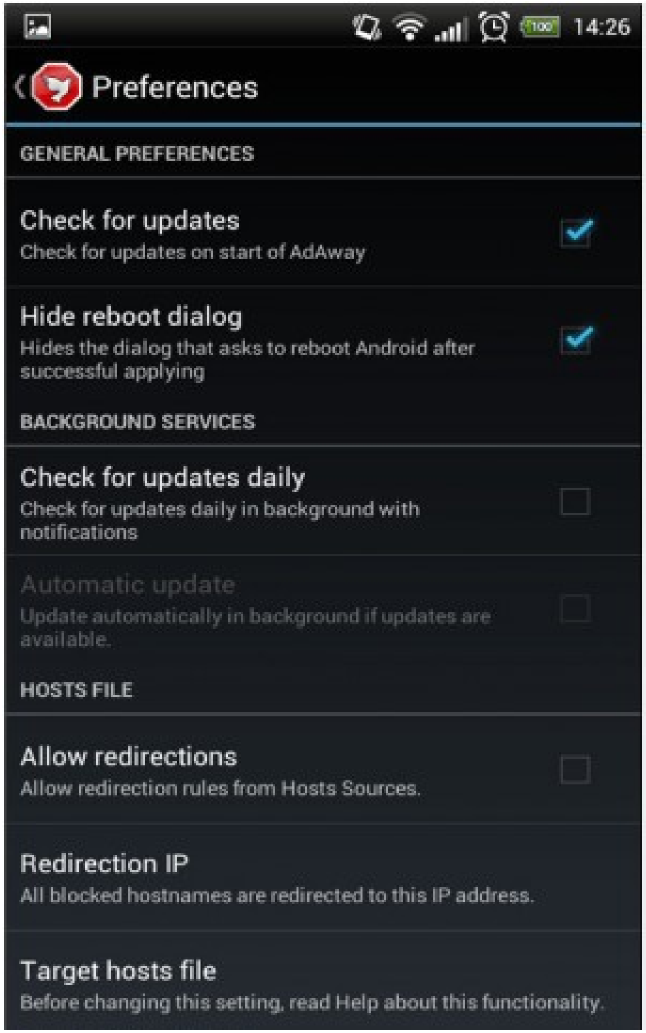
File name: update.zip

- ☑ Accounts
- ☑ AccuWeather 2.1.5
- ☑ Adobe Flash Player 11.1 11.1.115.12
- ☑ AfterFocus 1.2.5
- ☑ AirDroid 1.1.0
- ☑ Alarm 1.3.5
- ☑ Amazon 2.1.0
- ☑ Analytics 1.1.4

Order by: app name

☐ Show enabled elements on top

Adaway



14:26

Preferences

GENERAL PREFERENCES

Check for updates ☑
Check for updates on start of AdAway

Hide reboot dialog ☑
Hides the dialog that asks to reboot Android after successful applying

BACKGROUND SERVICES

Check for updates daily □
Check for updates daily in background with notifications

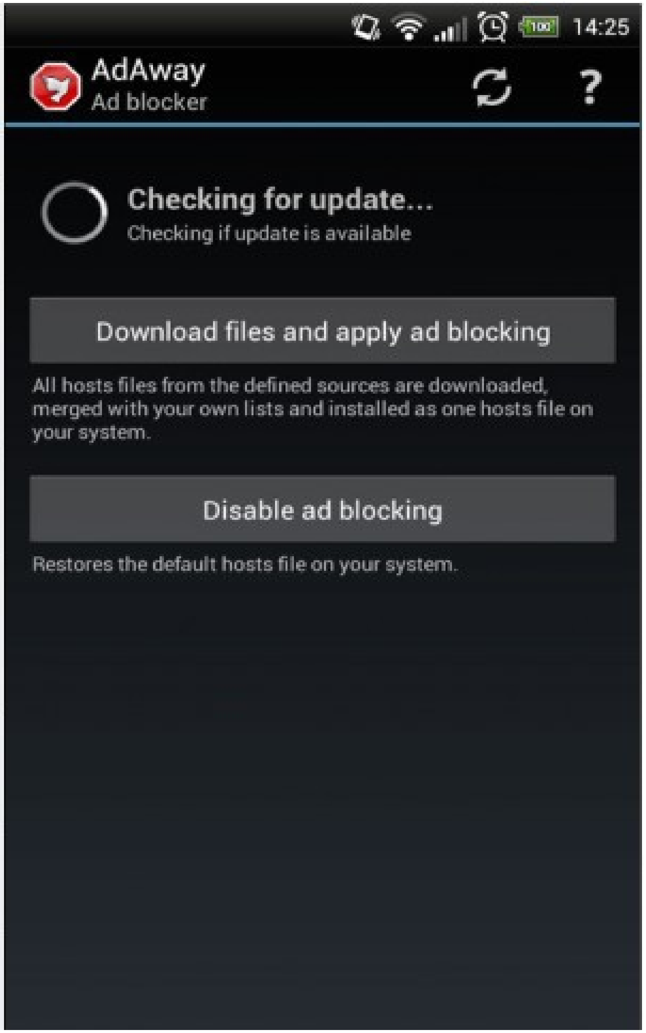
Automatic update □
Update automatically in background if updates are available.

HOSTS FILE

Allow redirections □
Allow redirection rules from Hosts Sources.

Redirection IP
All blocked hostnames are redirected to this IP address.

Target hosts file
Before changing this setting, read Help about this functionality.



14:25

AdAway
Ad blocker

Checking for update...
Checking if update is available

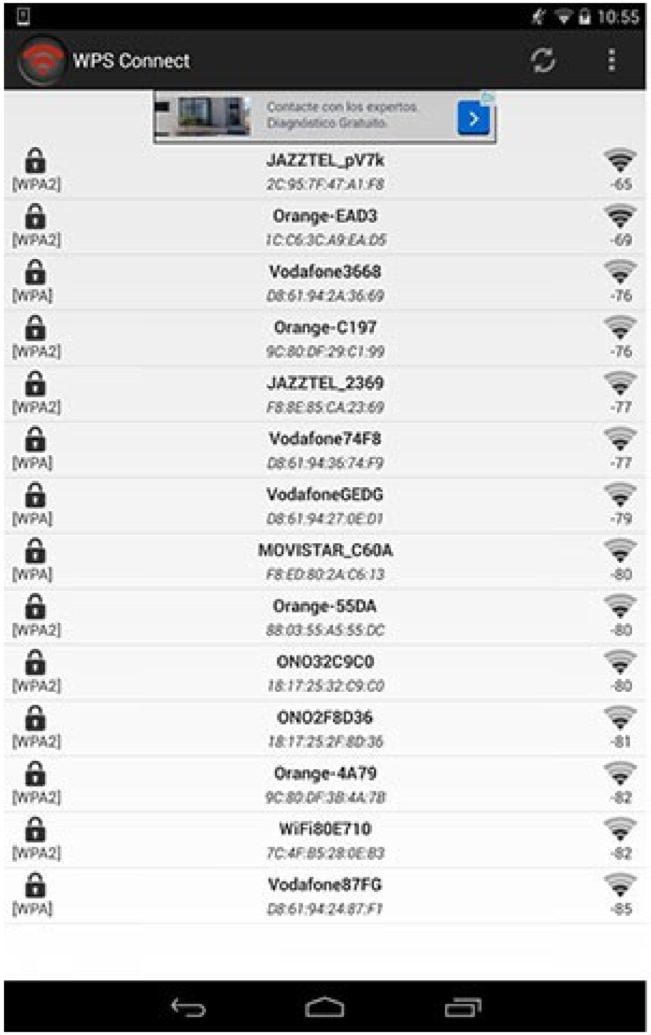
Download files and apply ad blocking

All hosts files from the defined sources are downloaded, merged with your own lists and installed as one hosts file on your system.

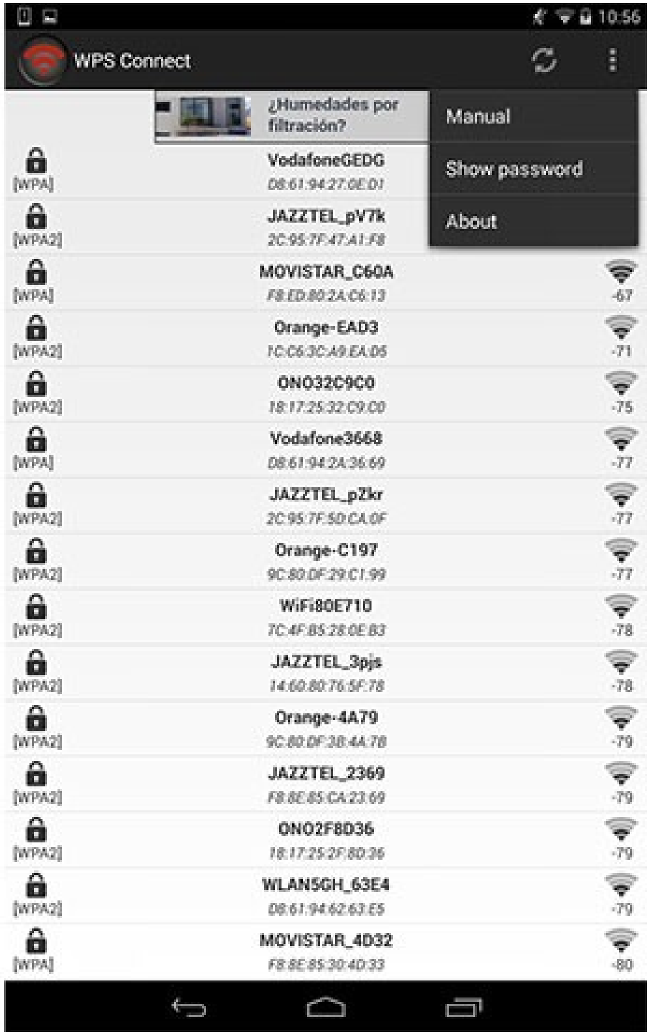
Disable ad blocking

Restores the default hosts file on your system.

WPS Connect

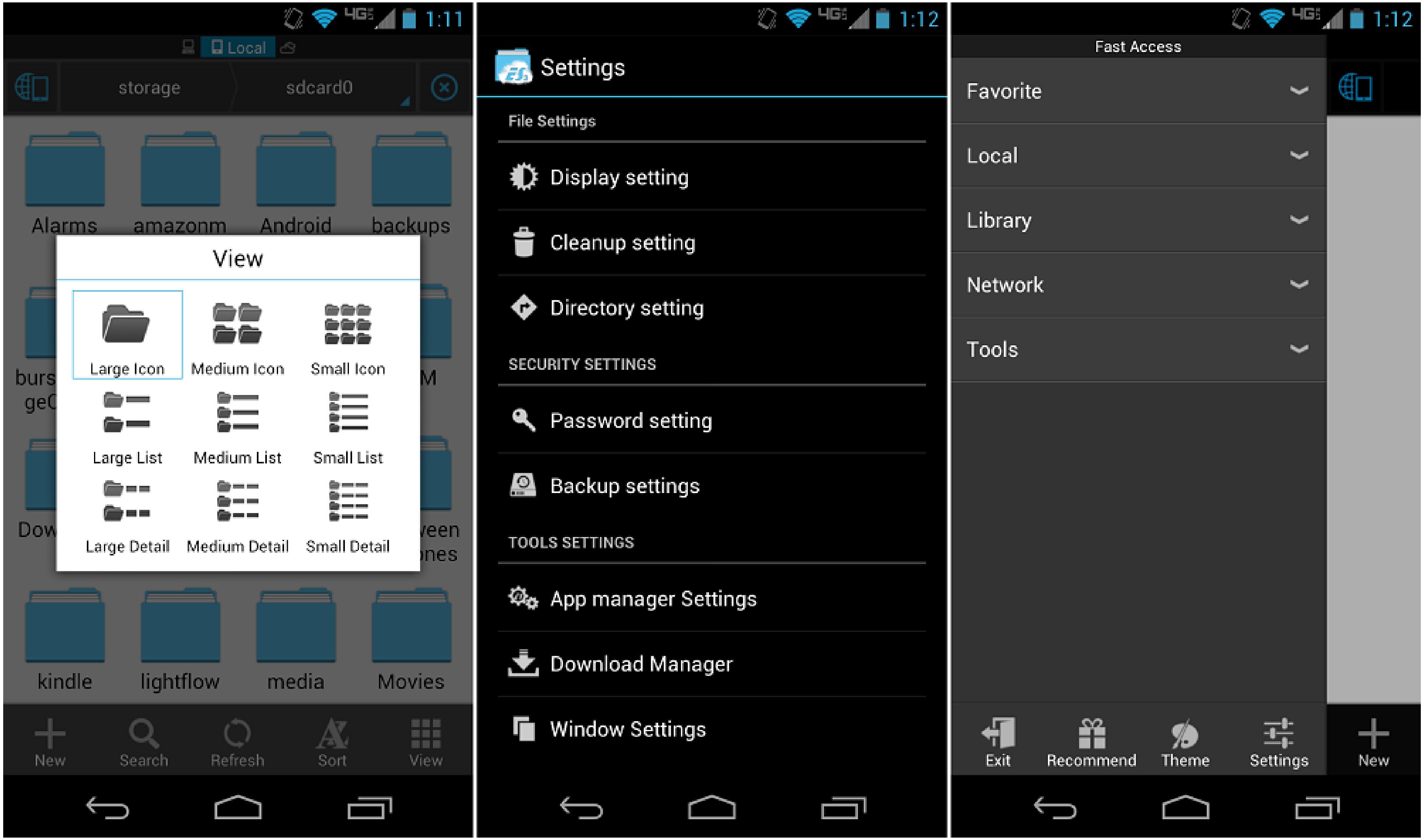


[WPA2]	JAZZTEL_pV7k	2C:95:7F:47:A1:F8	-65
[WPA2]	Orange-EAD3	1C:C6:3C:A9:EA:D5	-69
[WPA]	Vodafone3668	D8:61:94:2A:36:69	-76
[WPA2]	Orange-C197	9C:80:DF:29:C1:99	-76
[WPA2]	JAZZTEL_2369	F8:8E:85:CA:23:69	-77
[WPA]	Vodafone74F8	D8:61:94:36:74:F9	-77
[WPA]	VodafoneGEDG	D8:61:94:27:0E:D1	-79
[WPA]	MOVISTAR_C60A	F8:ED:80:2A:C6:13	-80
[WPA2]	Orange-55DA	88:03:55:A5:55:DC	-80
[WPA2]	ONO32C9C0	18:17:25:32:C9:C0	-80
[WPA2]	ONO2F8D36	18:17:25:2F:8D:36	-81
[WPA2]	Orange-4A79	9C:80:DF:38:4A:78	-82
[WPA2]	WiFi80E710	7C:4F:B5:28:0E:83	-82
[WPA]	Vodafone87FG	D8:61:94:24:87:F1	-85

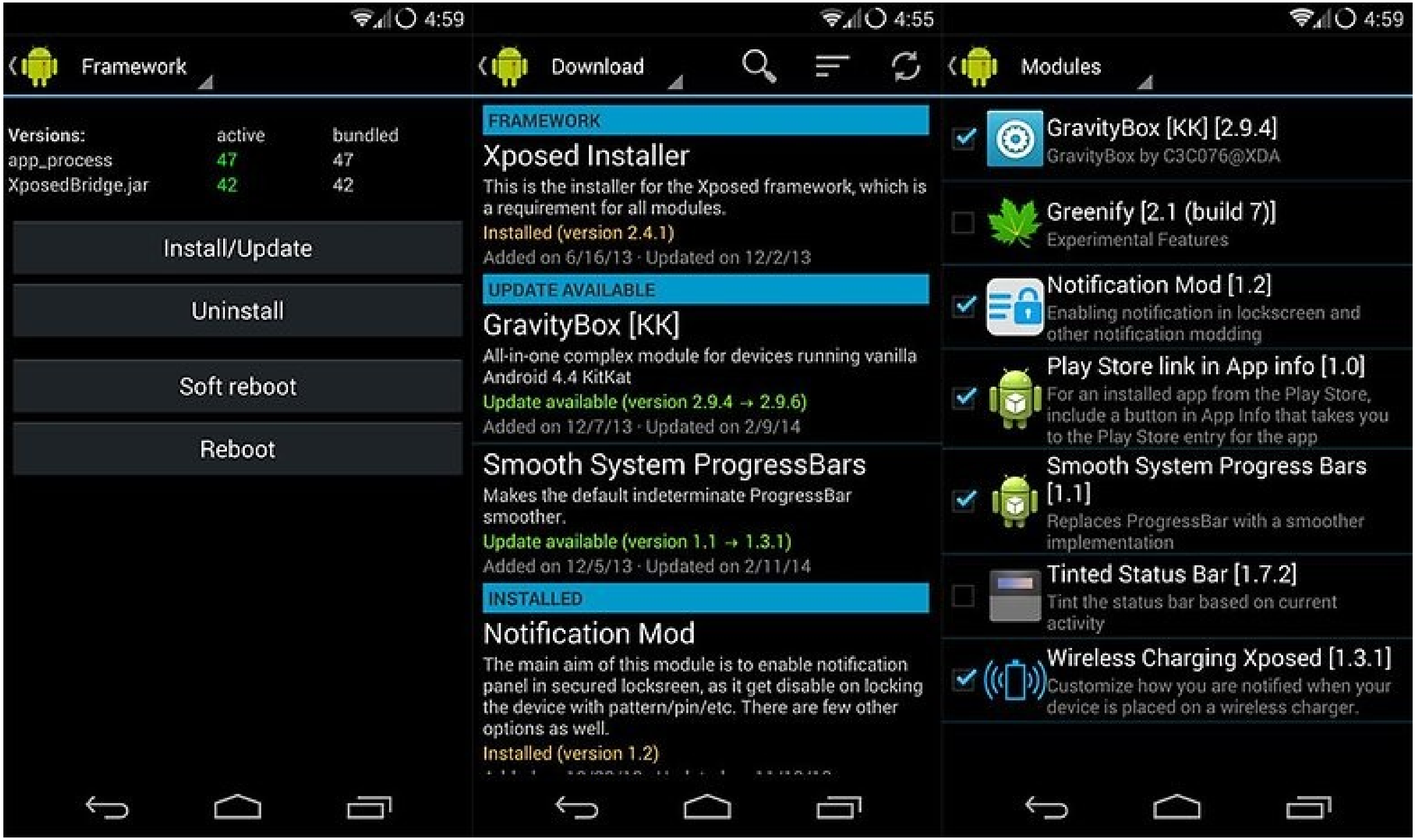


[WPA]	VodafoneGEDG	D8:61:94:27:0E:D1	
[WPA2]	JAZZTEL_pV7k	2C:95:7F:47:A1:F8	
[WPA]	MOVISTAR_C60A	F8:ED:80:2A:C6:13	-67
[WPA2]	Orange-EAD3	1C:C6:3C:A9:EA:D5	-71
[WPA2]	ONO32C9C0	18:17:25:32:C9:C0	-75
[WPA]	Vodafone3668	D8:61:94:2A:36:69	-77
[WPA2]	JAZZTEL_pZkr	2C:95:7F:50:CA:0F	-77
[WPA2]	Orange-C197	9C:80:DF:29:C1:99	-77
[WPA2]	WiFi80E710	7C:4F:B5:28:0E:83	-78
[WPA2]	JAZZTEL_3pjs	14:60:80:76:5F:78	-78
[WPA2]	Orange-4A79	9C:80:DF:38:4A:78	-79
[WPA2]	JAZZTEL_2369	F8:8E:85:CA:23:69	-79
[WPA2]	ONO2F8D36	18:17:25:2F:8D:36	-79
[WPA2]	WLAN5GH_63E4	D8:61:94:62:63:E5	-79
[WPA]	MOVISTAR_4D32	F8:8E:85:30:4D:33	-80

It's File Explorer



Xposed



Versions:	active	bundled
app_process	47	47
XposedBridge.jar	42	42

FRAMEWORK

Xposed Installer

This is the installer for the Xposed framework, which is a requirement for all modules.

Installed (version 2.4.1)

Added on 6/16/13 · Updated on 12/2/13

UPDATE AVAILABLE

GravityBox [KK]

All-in-one complex module for devices running vanilla Android 4.4 KitKat

Update available (version 2.9.4 → 2.9.6)

Added on 12/7/13 · Updated on 2/9/14

Smooth System ProgressBars

Makes the default indeterminate ProgressBar smoother.

Update available (version 1.1 → 1.3.1)

Added on 12/5/13 · Updated on 2/11/14

INSTALLED

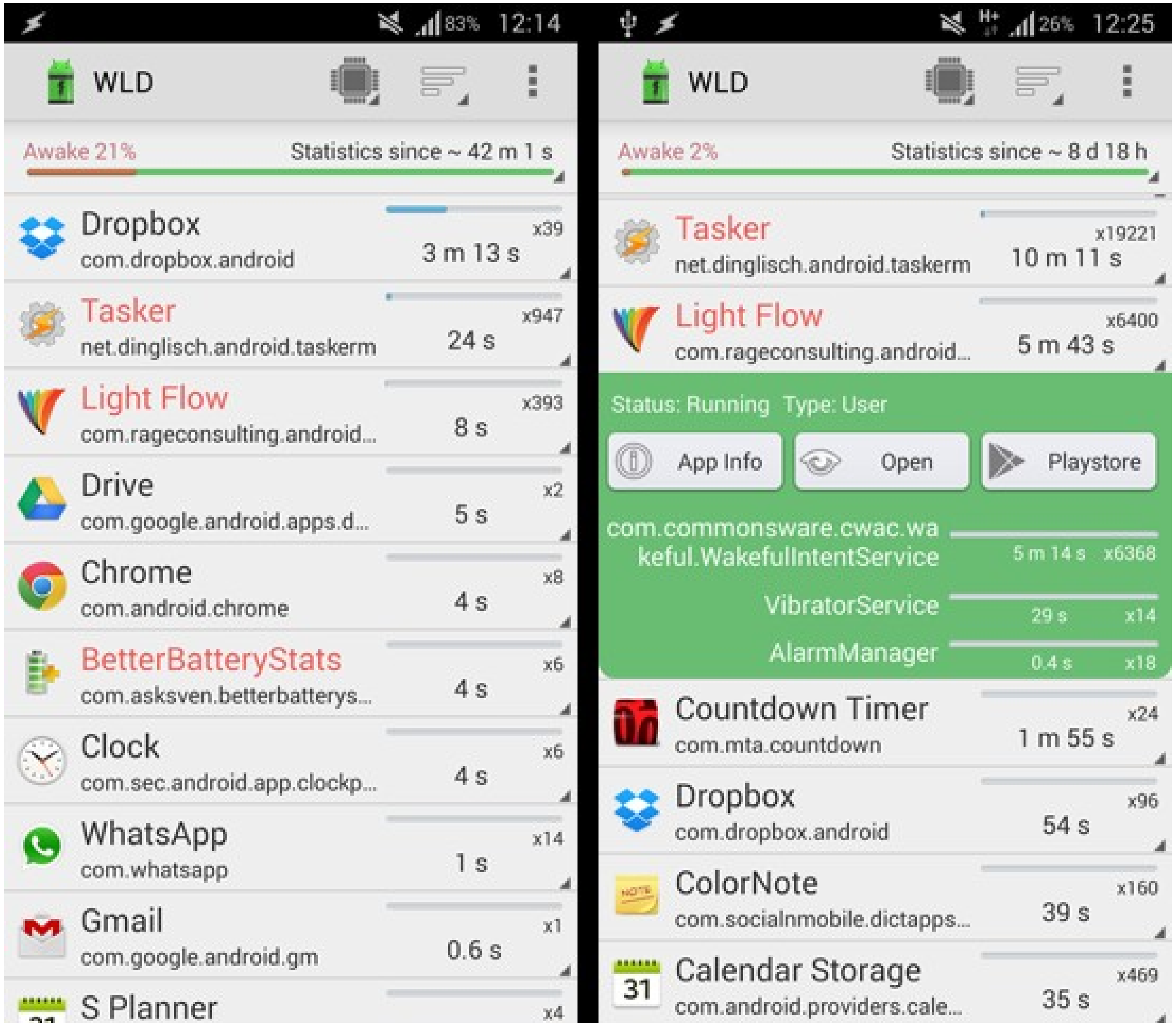
Notification Mod

The main aim of this module is to enable notification panel in secured locksreen, as it get disable on locking the device with pattern/pin/etc. There are few other options as well.

Installed (version 1.2)

- ☑ GravityBox [KK] [2.9.4]
  GravityBox by C3C076@XDA
- □ Greenify [2.1 (build 7)]
  Experimental Features
- ☑ Notification Mod [1.2]
  Enabling notification in lockscreen and other notification modding
- ☑ Play Store link in App info [1.0]
  For an installed app from the Play Store, include a button in App Info that takes you to the Play Store entry for the app
- ☑ Smooth System Progress Bars [1.1]
  Replaces ProgressBar with a smoother implementation
- □ Tinted Status Bar [1.7.2]
  Tint the status bar based on current activity
- ☑ Wireless Charging Xposed [1.3.1]
  Customize how you are notified when your device is placed on a wireless charger.

wakelock Detector



83% 12:14

WLD

Awake 21% Statistics since ~ 42 m 1 s

Dropbox com.dropbox.android	x39	3 m 13 s
Tasker net.dinglisch.android.taskerm	x947	24 s
Light Flow com.rageconsulting.android...	x393	8 s
Drive com.google.android.apps.d...	x2	5 s
Chrome com.android.chrome	x8	4 s
BetterBatteryStats com.asksven.betterbatterys...	x6	4 s
Clock com.sec.android.app.clockp...	x6	4 s
WhatsApp com.whatsapp	x14	1 s
Gmail com.google.android.gm	x1	0.6 s
S Planner	x4	

26% 12:25

WLD

Awake 2% Statistics since ~ 8 d 18 h

Tasker net.dinglisch.android.taskerm	x19221	10 m 11 s
Light Flow com.rageconsulting.android...	x6400	5 m 43 s

Status: Running Type: User

App Info Open Playstore

com.commonsware.cwac.wakeful.WakefulIntentService	5 m 14 s	x6368
VibratorService	29 s	x14
AlarmManager	0.4 s	x18

Countdown Timer com.mta.countdown	x24	1 m 55 s
Dropbox com.dropbox.android	x96	54 s
ColorNote com.socialnmobile.dictapps...	x160	39 s
Calendar Storage com.android.providers.cale...	x469	35 s

demo OnePlus 3

https://www.youtube.com/watch?v=BYX3ciuQvQ0

demo OnePlus 3

- **0: 48-2: 10** Download files necessary
- **2: 11-3: 00** Installation adb
- **3: 01-4: 10** Installing drivers phone
- **4: 11-5: 00** unlocking bootloader
- **5: 01-6: 45** Copying files (ROM + SuperSU) to tlf + Install TWRP
- **6: 46-8: 25** Enters and install TWRP ROM + Root
- **8: 26-9: 16** ROM Setup Wizard "rooteada"

uc3m | Universidad Carlos III de Madrid

Grupo de investigación:
Computer Security Lab

Mobile Devices Security

Degree in Computer Engineering

2019