iDevice Restore Process

How to restore firmware on iphone/ ipad/itouch

iDevice

- iPhone
  - iPhone3GS
  - iPhone4
- iPad
  - iPad
  - iPad2
- iTouch

iDevice	Firmware
iPhone	
iPhone3GS	iPhone2,1_*.ipsw
iPhone4	iPhone3,1_*.ipsw
iPad	
iPad	iPad1,1_*.ipsw
iPad2	iPad2,1_*.ipsw
iTouch	iPad4,1_*.ipsw

iTunes

- iTunes
- Usbmuxd

  /System/Library/PrivateFrameworks/MobileDevice.framework/Versions/A/Resources/usbmuxd &
- AFC2

  Apple File Connection
- ASR

  Apple Software Recovery
- Sqlite3
- SSL
- Obfuscate & AES

Firmware

- ipsw
- dmg
- img3
- kernelcache
- iBEC
- iBSS
- iBoot
- LLB

ipsw

- Unzip –d

dmg

RootFS	038-2191-001.dmg
Update Ramdisk	038-2170-001.dmg
Restore Ramdisk	038-2169-001.dmg

Img3

http://theiphonewiki.com/wiki/index.php?title=IMG3_File_Format

- Header
- Element
  - SHSH
- ElementHeader

Img3 Tags

- VERS: iBoot version of the image
- SEPO: Security Epoch
- SDOM: Security Domain
- PROD: Production Mode
- CHIP: Chip to be used with. example: "0x8900" for S5L8900.
- BORD: Board to be used with
- KBAG: contains the KEY and IV required to decrypt encrypted with the GID-key
- SHSH: RSA encrypted SHA1 hash of the file
- CERT: Certificate
- ECID: Exclusive Chip ID unique to every device with iPhone OS.
- TYPE: Type of image, should contain the same string as 'iden' of the header
- DATA: Real content of the file

iBSS

Uploaded via DFU to bootstrap iBEC during DFU Mode restore

iBEC

Uploaded when performing a restore from Fake DFU in LLB

Boot sequence

http://code.google.com/p/chronicdev/wiki/BootSequence

- Bootrom
- LLB
- iBoot
- Ramdisk
- Kernel

iBSS

iBEC

iDevice mode

- Normal
- DFU mode

    Device Firmware Upgrade

- Recovery mode
- Restore mode

Device information

- ECID
  UniqueChipID/Exclusive Chip ID
- BasebandVersion
- ICCID
  IntegratedCircuitCardIdentity
- IMEI
  InternationalMobileEquipmentIdentity
- IMSI
  MCC, MNC, MSIN
- SerialNumber
- CPUArchitecture
- ModelNumber
- HardwarePlatform

Firmware patch

- TSS

  http://gs.apple.com/TSS/controller?action=2

- SHSH

  Blob

Recovery mode

- iBEC
- go
- ramdisk
- deviceTree
- kernelCache
- bootargs

```
    setenv boot-args rd=md0 nand-enable-reformat=1 –progress
```

- boot

Restoring…

- Start restoring
- ASR
  - SystemImageData
  - NORData
    - NorImageData
    - LlbImageData
  - KernelCacheFile

Restore Progress

- 11 => "Waiting for storage device",
- 12 => "Creating partition map",
- 13 => "Creating filesystem",
- 14 => "Restoring image",
- 15 => "Verifying restore",
- 16 => "Checking filesystems",
- 17 => "Mounting filesystems",
- 19 => "Flashing NOR",
- 20 => "Updating baseband",
- 21 => "Finalizing NAND epoch update",
- 26 => "Modifying persistent boot-args",
- 27 => "Unmounting filesystems",
- 28 => "Partition NAND device",
- 29 => "Waiting for NAND",
- 30 => "Waiting for device",
- 33 => "Loading kernelcache",
- 36 => "Loading NOR data to flash",

Activate

- Device Information
  - UniqueDeviceID
  - IMEI
  - ICCID
  - SerialNumber
  - IMSI
- Fetching record

  https://albert.apple.com/WebObjects/ALUnbrick.woa/wa/deviceActivation"
- Activation
  - AccountToken
  - AccountTokenCertificate
  - AccountTokenSignature
  - DeviceCertificate
  - FairPlayKeyData

Others

- IPA installation
- Syncing PIM
- AFC2
- Syslog
- Screenshot
- Developer Profile

Tools

- ruby
- socat
- libusb
- unzip
- ribUsb
- bit-struct
- CFPropertyList

Other tools on win32

- VirtualBox/VmWare
- Cygwin
- s-irecovery

Thanks

- chronic-dev, redsn0w
- saurik,comet, posixninja, iH8sn0w
- http://theiphonewiki.com/
- libimobiledevice
- libirecovery
- libplist
- libusbmuxd
- idevicerestore
- ideviceactivate
- ideviceinstaller

Questions

- ?
- ??
- ???

Todo

- S-irecovery on win32
- DFU
- FOTA